PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-187836
(43)Date of publication of application : 21.07.1998

(51)Int.Cl. G06F 17/60
G09C 1/00

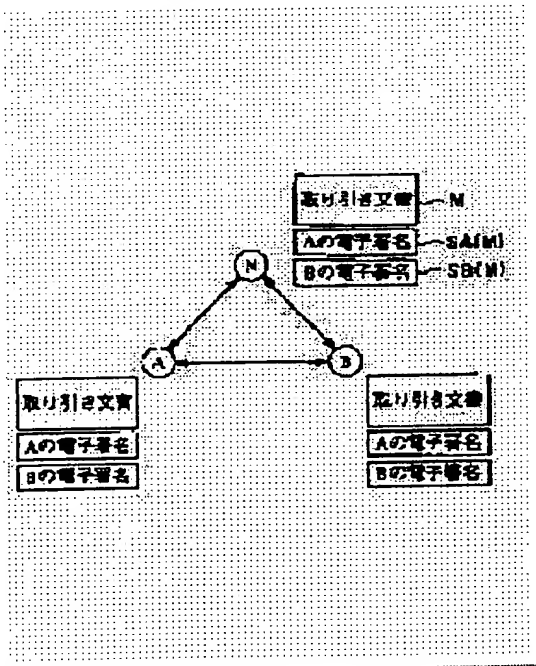
(21)Application number : 09-292921
(22)Date of filing : 24.10.1997

(71)Applicant : FUJITSU LTD
(72)Inventor : KURODA YASUTSUGU
KOMURA MASAHIRO
TORII SATORU
IWASE SHIYOUKO
ONO KOSHIO

(30)Priority
Priority number : 08288539 Priority date : 30.10.1996 Priority country : JP

(54) DEVICE AND METHOD FOR PROVING TRANSACTION IN NETWORK ENVIRONMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To guarantee the safety of transaction to be performed between users while utilizing a communication network.
SOLUTION: A transaction document M describing the contents of transaction between users A and B is prepared and an electronic signature SA(M) of user A and an electronic signature SB(M) of user B for that document are prepared. Then, these signatures are sent to the notarial act equipment of notarial person N together with the transaction document M and the users A and B and the notarial person N share information. Thus, the notarial person N can objectively prove the contents, etc., of transaction.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10187836 A**

(43) Date of publication of application: **21 . 07 . 98**

(51) Int. Cl **G06F 17/60**
G09C 1/00

(21) Application number: **09292921**

(22) Date of filing: **24 . 10 . 97**

(30) Priority: **30 . 10 . 96 JP 08288539**

(71) Applicant: **FUJITSU LTD**

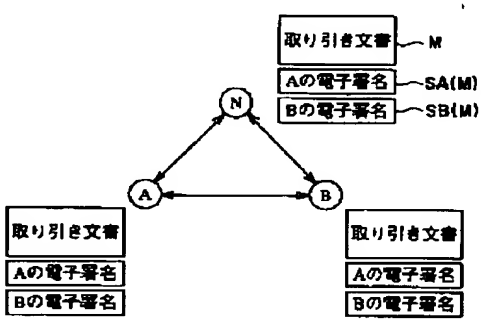
(72) Inventor: **KURODA YASUTSUGU**
KOMURA MASAHIRO
TORII SATORU
IWASE SHIYOUKO
ONO KOSHIO

(54) DEVICE AND METHOD FOR PROVING TRANSACTION IN NETWORK ENVIRONMENT

(57) Abstract:

PROBLEM TO BE SOLVED: To guarantee the safety of transaction to be performed between users while utilizing a communication network.

SOLUTION: A transaction document M describing the contents of transaction between users A and B is prepared and an electronic signature SA(M) of user A and an electronic signature SB(M) of user B for that document are prepared. Then, these signatures are sent to the notarial act equipment of notarial person N together with the transaction document M and the users A and B and the notarial person N share information. Thus, the notarial person N can objectively prove the contents, etc., of transaction.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－187836

(43)公開日　平成10年(1998)７月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３３０
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｂ

審査請求　未請求　請求項の数25　ＯＬ　（全 26 頁）

(21)出願番号　特願平9－292921

(22)出願日　平成９年(1997)10月24日

(31)優先権主張番号　特願平8－288539

(32)優先日　平８(1996)10月30日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　黒田　康嗣
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　小村　昌弘
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

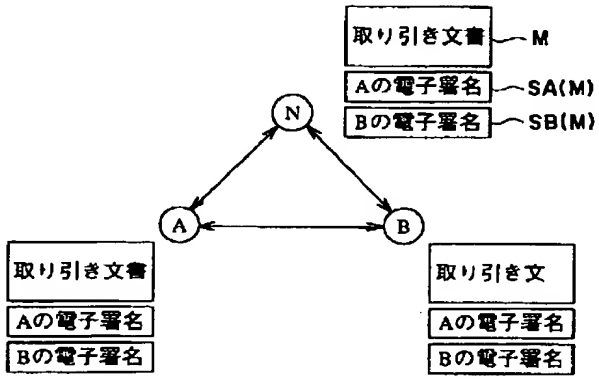
(74)代理人　弁理士　大菅　義之　（外１名）

最終頁に続く

(54)【発明の名称】　ネットワーク環境における取り引き証明装置および方法

(57)【要約】
【課題】　ユーザ間で行われる取り引きの安全性を、通信ネットワークを利用して保証することが課題である。
【解決手段】　ユーザＡとユーザＢの取り引きの内容を記述した取り引き文書Ｍを作成し、それに対するユーザＡの電子署名ＳＡ（Ｍ）およびユーザＢの電子署名ＳＢ（Ｍ）を作成する。そして、それらを取り引き文書Ｍとともに公証人Ｎの公証装置に送り、ユーザＡ、Ｂ、および公証人Ｎが情報を共有する。こうして、第３者である公証人Ｎが、取り引きの内容等を客観的に証明することができる。

内容保証サービスにおける共有情報を示す図



1

【特許請求の範囲】

【請求項１】　複数のユーザ間で行われる取り引きに関する情報処理を行う取り引き証明装置であって、
通信ネットワークに接続され、第１のユーザと第２のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第１のユーザの電子署名データと第２のユーザの電子署名データとを、該ネットワークから受け取る通信手段と、
前記第１のユーザの電子署名データと第２のユーザの電子署名データを検証する処理手段と、
前記第１のユーザの電子署名データと第２のユーザの電子署名データを記憶する記憶手段とを備えることを特徴とする取り引き証明装置。

【請求項２】　前記通信手段は、前記ネットワークから前記取り引き文書データをさらに受け取り、前記処理手段は、該取り引き文書データを用いて前記第１のユーザの電子署名データと第２のユーザの電子署名データを検証し、該取り引き文書データを、該第１のユーザの電子署名データと第２のユーザの電子署名データとともに前記記憶手段に格納することを特徴とする請求項１記載の取り引き証明装置。

【請求項３】　取り引き日時を表す日時情報を発行する日時発行手段をさらに備え、前記通信手段は、日時情報を含む前記取り引き文書データを受け取り、前記処理手段は、該取り引き文書データに含まれる日時情報が前記日時発行手段が発行した日時情報と一致するかどうかを確認することを特徴とする請求項２記載の取り引き証明装置。

【請求項４】　取り引きの識別子情報を発行する識別子発行手段をさらに備え、前記通信手段は、識別子情報を含む前記取り引き文書データを受け取り、前記処理手段は、該取り引き文書データに含まれる識別子情報が前記識別子発行手段が発行した識別子情報と一致するかどうかを確認することを特徴とする請求項２記載の取り引き証明装置。

【請求項５】　前記記憶手段は、前記第１のユーザおよび第２のユーザが保存している第１のユーザの電子署名データ、第２のユーザの電子署名データ、および取り引き文書データと共通の前記第１のユーザの電子署名データ、第２のユーザの電子署名データ、および取り引き文書データを記憶することを特徴とする請求項２記載の取り引き証明装置。

【請求項６】　前記通信手段は、前記ネットワークから前記取り引き文書データの参照要求を受け取り、前記処理手段は、該参照要求に応じて該取り引き文書データを前記記憶手段から取り出し、該通信手段は、該取り引き文書データの内容を、該ネットワークを介して要求元に送ることを特徴とする請求項２記載の取り引き証明装置。

【請求項７】　前記処理手段は、前記第１のユーザの電

2

子署名データと第２のユーザの電子署名データの少なくとも一方を含むデータに第３者の電子署名を施し、第３者の電子署名データを生成して、該第３者の電子署名データを前記記憶手段に格納することを特徴とする請求項１記載の取り引き証明装置。

【請求項８】　前記通信手段は、前記第３者の電子署名データを、前記ネットワークを介して前記第１のユーザおよび第２のユーザに送ることを特徴とする請求項７記載の取り引き証明装置。

【請求項９】　前記通信手段は、前記ネットワークから前記取り引き文書データに対する合意者の電子署名をさらに受け取り、該合意者の電子署名を前記第１のユーザの電子署名データと第２のユーザの電子署名データとともに前記記憶手段に格納することを特徴とする請求項１記載の取り引き証明装置。

【請求項１０】　前記通信手段は、暗号化された前記第１のユーザの電子署名データと第２のユーザの電子署名データとを受け取り、前記処理手段は、該暗号化された第１のユーザの電子署名データと第２のユーザの電子署名データを復号化してから検証することを特徴とする請求項１記載の取り引き証明装置。

【請求項１１】　複数のユーザ間で行われる取り引きに関する情報処理を行う取り引き証明装置であって、
通信ネットワークに接続され、第１のユーザと第２のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第１のユーザの電子署名データに対して作成された第２のユーザの電子署名データを、該ネットワークから受け取る通信手段と、
前記第２のユーザの電子署名データを検証する処理手段と、
前記第２のユーザの電子署名データを記憶する記憶手段とを備えることを特徴とする取り引き証明装置。

【請求項１２】　複数のユーザ間で行われる取り引きに関する情報処理を行う取り引き証明装置であって、
通信ネットワークに接続され、第１のユーザと第２のユーザの間の取り引きに関する事項を記述した第１のユーザの取り引き情報と第２のユーザの取り引き情報とを、該ネットワークから受け取る通信手段と、
前記第１のユーザの取り引き情報と第２のユーザの取り引き情報の内容が同じであることを確認する処理手段と、
前記取り引き情報を記憶する記憶手段とを備えることを特徴とする取り引き証明装置。

【請求項１３】　複数のユーザ間で行われる取り引きに関する情報処理を行う端末装置であって、
第１のユーザと第２のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第１のユーザの電子署名データを作成する処理手段と、
通信ネットワークに接続され、前記第１のユーザの電子署名データを該ネットワークを介して第３者に送信し、

前記取り引き文書データに対する第２のユーザの電子署名データであって、該第３者により検証された該第２のユーザの電子署名データを、該第３者から該ネットワークを介して受信する通信手段と、

前記第１のユーザの電子署名データと第２のユーザの電子署名データを記憶する記憶手段とを備えることを特徴とする端末装置。

【請求項１４】　前記通信手段は、前記第３者に前記ネットワークを介して前記取り引き文書データをさらに送信し、前記第３者により該取り引き文書データを用いて検証された前記第２のユーザの電子署名データを受信し、該取り引き文書データを、前記第１のユーザの電子署名データと第２のユーザの電子署名データとともに前記記憶手段に格納することを特徴とする請求項１３記載の端末装置。

【請求項１５】　複数のユーザ間で行われる取り引きに関する情報処理を行う端末装置であって、

第１のユーザと第２のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第１のユーザの電子署名データを作成する処理手段と、

通信ネットワークに接続され、前記取り引き文書データに対する第２のユーザの電子署名データを前記第２のユーザから該ネットワークを介して受信し、前記第１のユーザの電子署名データと第２のユーザの電子署名データを、該ネットワークを介して第３者に送信する通信手段と、

前記第１のユーザの電子署名データと第２のユーザの電子署名データを記憶する記憶手段とを備えることを特徴とする端末装置。

【請求項１６】　前記通信手段は、前記第１のユーザの電子署名データと第２のユーザの電子署名データの少なくとも一方を含むデータに対する前記第３者の電子署名データを、前記ネットワークから受信し、前記処理手段は、該第３者の電子署名データを検証して前記記憶手段に格納することを特徴とする請求項１３または１５記載の端末装置。

【請求項１７】　複数のユーザ間で行われる取り引きに関する情報処理を行う端末装置であって、

第１のユーザと第２のユーザの間の取り引きに関する事項を記述した第１のユーザの取り引き情報を作成する処理手段と、

通信ネットワークに接続され、前記第１のユーザの取り引き情報を該ネットワークを介して第３者に送信し、該第３者により第２のユーザの取り引き情報と内容が同じであることを確認された該第１のユーザの取り引き情報を、該第３者から該ネットワークを介して受信する通信手段と、

受信した取り引き情報を記憶する記憶手段とを備えることを特徴とする端末装置。

【請求項１８】　複数のユーザ間で行われる取り引きに関する情報処理を行う端末装置であって、

第１のユーザと第２のユーザの間の取り引きに関する事項を記述した第１のユーザの取り引き情報を作成する処理手段と、

通信ネットワークに接続され、前記第２のユーザの取り引き情報を前記第２のユーザから該ネットワークを介して受信し、前記第１のユーザの取り引き情報と第２のユーザの取り引き情報を、該ネットワークを介して第３者に送信する通信手段と、

前記第１のユーザの取り引き情報を記憶する記憶手段とを備えることを特徴とする端末装置。

【請求項１９】　複数のユーザ間で行われる取り引きに関する情報処理を行う取り引き証明システムであって、

第１のユーザと第２のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第１のユーザの電子署名データを作成する作成手段と、

前記取り引き文書データに対する第２のユーザの電子署名データを作成する作成手段と、

通信ネットワークに接続され、前記第１のユーザの電子署名データと第２のユーザの電子署名データとを、該ネットワークから受け取る通信手段と、

前記第１のユーザの電子署名データと第２のユーザの電子署名データを検証する処理手段と、

前記第１のユーザにより参照され、前記第１のユーザの電子署名データと第２のユーザの電子署名データを記憶する第１の記憶手段と、

前記第２のユーザにより参照され、前記第１のユーザの電子署名データと第２のユーザの電子署名データを記憶する第２の記憶手段と、

第３者により参照され、前記第１のユーザの電子署名データと第２のユーザの電子署名データを記憶する第３の記憶手段と

を備えることを特徴とする取り引き証明システム。

【請求項２０】　前記第１のユーザの電子署名データと第２のユーザの電子署名データの少なくとも一方を含むデータに対する前記第３者の電子署名データを作成する作成手段をさらに備え、前記処理手段は、該第３者の電子署名データを検証し、前記第１、第２、および第３の記憶手段は、該第３者の電子署名データをさらに記憶することを特徴とする請求項１９記載の取り引き証明システム。

【請求項２１】　複数のユーザ間で行われる取り引きに関する情報処理を行うコンピュータのためのプログラムを記録した記録媒体であって、

第１のユーザと第２のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第１のユーザの電子署名データと第２のユーザの電子署名データとを、通信ネットワークから受け取る機能と、

前記第１のユーザの電子署名データと第２のユーザの電子署名データを検証する機能と、

前記第１のユーザの電子署名データと第２のユーザの電子署名データを記憶する機能と
を前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２２】　複数のユーザ間で行われる取り引きに関する情報処理を行うコンピュータのためのプログラムを記録した記録媒体であって、
第１のユーザと第２のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第１のユーザの電子署名データを作成する機能と、
前記第１のユーザの電子署名データを通信ネットワークを介して第３者に送信し、前記取り引き文書データに対する第２のユーザの電子署名データであって、該第３者により検証された該第２のユーザの電子署名データを、該第３者から該ネットワークを介して受信する機能と、
前記第１のユーザの電子署名データと第２のユーザの電子署名データを記憶する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２３】　複数のユーザ間で行われる取り引きに関する情報処理を行うコンピュータのためのプログラムを記録した記録媒体であって、
第１のユーザと第２のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第１のユーザの電子署名データを作成する機能と、
前記取り引き文書データに対する第２のユーザの電子署名データを前記第２のユーザから通信ネットワークを介して受信し、前記第１のユーザの電子署名データと第２のユーザの電子署名データを、該ネットワークを介して第３者に送信する機能と、
前記第１のユーザの電子署名データと第２のユーザの電子署名データを記憶する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２４】　複数のユーザ間で行われる取り引きに関する情報処理を行う取り引き証明方法であって、
第１のユーザと第２のユーザの間の取り引きに関する事項を記述した取り引き文書データを作成し、
前記取り引き文書データに対する第１のユーザの電子署名データと第２のユーザの電子署名データを作成し、
前記第１のユーザの電子署名データと第２のユーザの電子署名データとを、通信ネットワークを介して第３者に送信し、
前記第１のユーザの電子署名データと第２のユーザの電子署名データを検証し、
前記第１のユーザの電子署名データと第２のユーザの電子署名データを保存することを特徴とする取り引き証明方法。

【請求項２５】　前記第１のユーザの電子署名データと第２のユーザの電子署名データの少なくとも一方を含むデータに対する前記第３者の電子署名データを作成し、該第３者の電子署名データを検証し、該第３者の電子署名データを保存することを特徴とする請求項２４記載の取り引き証明方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、２以上の当事者間で行われる取り引きの内容等の取り引きに関する事項を、通信ネットワークを利用して客観的に証明する取り引き証明装置およびその方法に関する。

【０００２】

【従来の技術】今日、インターネットやパーソナルコンピュータの普及に伴い、通信ネットワークを介してコンピュータ間で様々な取り引きが行われつつある。しかし、インターネットには基本的に誰でも自由にアクセスすることができるため、通信相手の本人確認が難しく、送信データが盗用されたり、改ざんされたりする恐れもある。

【０００３】このため、ネットワーク環境において本格的な商取り引きを行うには、このような不正行為を防止する工夫が必要不可欠となる。従来の不正行為防止方法には、例えば次のようなものがある。

（ａ）電子取引方式（特開昭６２－０５６０４３）
署名者が自分の電子署名（電子捺印）を作成する際、認証用データの定まった位置に電子署名の猶予期限を示す日付データを付加する。これにより、電子署名を受信した認証者に対して応答の期限を明示し、期限までに応答がない場合、取り引きが中止となり、送信した電子署名が無効になることを宣言する。

【０００４】署名者は、猶予期限を過ぎても応答が得られない場合、その事実を電子署名とともに公証機関に届けることによって電子署名を無効にできるようにする。これにより、電子署名の認証者が応答を返さずに持ち逃げした場合や認証者が不正な署名を送信した場合でも、電子署名の悪用を防止できる。

（ｂ）電子的公証方法および装置（特開平０６－０１４０１８）
データが真正であることの証明を希望する当事者からデータが電子的公証装置に供給されると、日時発生器は、当事者が変更できないある時点を指定する日時情報を発生する。そして、データの内容と日時情報が暗号器により暗号化され、日時が印字された真正証明データが公証装置から出力される。これにより、文書または電子的に記録されたデータが、印字された日時以降変更されなかったことが確認でき、文書の真正性を電子的に公証することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、上述のような従来の不正行為防止方法には次のような問題がある。

【０００６】電子取引方式によれば、電子署名の有効期限を取り引き相手に通知して、その悪用を防止することができる。しかし、これにより、取り引き相手の確認を行ったり、取り引き内容の改ざんを防止したりすることはできない。

【０００７】また、電子的公証方法によれば、公証装置が文書に日時情報を付加することで、その真正性を電子的に公証することができる。しかし、この公証装置は、単独の当事者が入力したデータの真正性を証明するため、入力前にデータが改ざんされたかどうかは判定することができない。したがって、２者間の取り引き文書等の場合、結果的に不正な内容が真正データとして出力される可能性がある。

【０００８】したがって、悪意のあるユーザが取り引き内容等を偽る可能性があり、ネットワークを利用した商取り引きが必ずしも安全に行われるとは限らないという問題がある。

【０００９】ところで、商品取り引き所における取り引きの管理形態は次のようなものである。先物売買などの商品の取り引きは、すべて商品取り引き所で行われる。取り引きの当事者は取り引き所の会員となり、あらかじめ一定金額の保証金を収めておく。そして、不正が行われた場合には、保証金が没収される。

【００１０】しかしながら、商品取り引き所における取り引きは、一般的な企業間取り引きとは異なっており、ネットワーク上の商取り引きにそのまま応用するのは困難である。

【００１１】本発明の課題は、２以上の当事者間で行われる取り引きの安全性を、通信ネットワークを利用して保証する取り引き証明装置およびその方法を提供することである。

【００１２】

【課題を解決するための手段】図１は、本発明の取り引き証明システムの原理図である。図１の取り引き証明システムは、取り引き証明装置１、第１のユーザの端末装置２、および第２のユーザの端末装置３を含み、複数のユーザ間で行われる取り引きに関する情報処理を行う。取り引き証明装置１と端末装置２、３は、通信ネットワーク４により互いに結合されている。

【００１３】端末装置２は、第１のユーザと第２のユーザの間の取り引きに関する事項を記述した取り引き文書データに対する第１のユーザの電子署名データ８を作成し、端末装置３は、その取り引き文書データに対する第２のユーザの電子署名データ９を作成する。これらの電子署名データ８、９は、ネットワーク４を介して、取り引き証明装置１に送信される。

【００１４】取り引き証明装置１は第３者の情報処理装置に相当し、通信手段５、処理手段６、および記憶手段７を備える。通信手段５は、ネットワーク４に接続され、第１のユーザの電子署名データ８と第２のユーザの電子署名データ９とをネットワーク４から受け取る。

【００１５】処理手段６は、第１のユーザの電子署名データ８と第２のユーザの電子署名データ９を検証し、記憶手段７は、第１のユーザの電子署名データ８と第２のユーザの電子署名データ９を記憶する。

【００１６】電子署名とは、データの送信者が本人しか知らない秘密鍵を用いて、なんらかの方法でデータを暗号化して作成した情報である。ここでは、第１のユーザの電子署名データ８は、第１のユーザの秘密鍵を用いて作成され、第２のユーザの電子署名データ９は、第２のユーザの秘密鍵を用いて作成される。

【００１７】ユーザの電子署名は、そのユーザ自身しか作成できないので、取り引き文書データにユーザの電子署名が施されると、取り引き内容がそのユーザにより承認されたものとみなされる。

【００１８】処理手段６は、通信手段５を介してこれらの電子署名データ８、９を受け取ると、第１のユーザの公開鍵、第２のユーザの公開鍵を用いて電子署名データ８、９をそれぞれ復号化し、それらの内容を検証する。

【００１９】両者の内容が同じであれば、第１および第２のユーザの双方が取り引きに合意したものとみなし、その証拠として電子署名データ８、９を記憶手段７に保存する。もし両者の内容が異なれば、その取り引きは不成立とみなして、端末装置２、３にエラー通知を行う。

【００２０】このように、取り引きの当事者とは異なる第３者の取り引き証明装置１が電子署名データ８、９を保管しておけば、取り引きが成立していることとその内容等を、いつでも他人に対して証明することが可能になる。したがって、取り引きの当事者である第１および第２のユーザは、取り引きに関する事項を偽ることが不可能になり、ネットワーク環境における取り引きの安全性が客観的に保証される。

【００２１】例えば、図１の取り引き証明装置１は、実施形態の図３における公証装置１１に対応し、通信手段５は図４におけるネットワーク接続装置２７に対応し、処理手段６はＣＰＵ２１（中央処理装置）とメモリ２２に対応し、記憶手段７はメモリ２２または外部記憶装置２５に対応する。

【００２２】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。商取り引きは、一般的に２人の当事者間の同意のもとに成り立つ。しかし、当事者同士が同意したことを客観的に証明するためには、“信頼のおける第三者（trusted third party）”が必要である。なぜなら、２者間のみの取り引きでは、一方がその事実を偽ることができるからである。

【００２３】本実施形態では、この“信頼のおける第三者”を“公証人（notary public）”または“notarization authority”と呼び、公証人がネットワーク環境での商取り引きを安全に行うことを保証する取り引き証明

システムを、取り引き公証システムと呼ぶことにする。

【００２４】ネットワーク環境で安全な商取り引きを行うには、取り引き公証システムが以下のようなサービスを提供する必要がある。

（１）身元保証サービス

公証人が、取り引きする相手の身元を保証する。これにより、偽りの取り引き相手を検出できる。

（２）日時保証サービス

公証人が、取り引きした日時を保証する。これにより、取り引きした日時を偽れなくなる。

（３）一意性保証サービス

公証人が、取り引きの一意性を保証する。これにより、他の取り引きとの混同が防止される。

（４）配達保証サービス

公証人が、取り引き情報が確実に配送されたことを保証する。これにより、取り引き情報の発信人が情報を発信したことを偽れなくなり、取り引き情報の受信人も情報を受信したことを偽れなくなる。また、取り引き情報が配送されなかった場合、どこで配送されなかったのかを検出できる。

（５）内容保証サービス

公証人が、取り引きの内容を保証する。これにより、内容が改ざんされたことを検出できる。また、必要に応じて、いつでも取り引き内容を参照できる。

（６）取り引き保証サービス

公証人が、特定の当事者同士が取り引きしたことを保証する。これにより、当事者が、取り引きしたことを偽れなくなる。

【００２５】図２は、ネットワーク上での２者間の商取り引き環境を示している。図２において、例えば、当事者Ａは取り引き情報の第１発信者であり、当事者Ｂはその取り引き情報の受信者である。当事者Ａ、Ｂは、互いにインターネット等の通信ネットワークを使って売買契約書等の取り引き情報を交換し、商取り引きを行っている。公証人Ｎは、当事者Ａ、Ｂとの間で個別に取り引き情報を交換して、それらを確認し、取り引きの安全性を保証する。

【００２６】図３は、図２のような商取り引き環境を実現するための取り引き公証システムの構成図である。図３の取り引き公証システムは、公証人Ｎの情報処理装置である公証装置１１、ユーザＡ、Ｂ、Ｃ、Ｄ、・・・の計算機端末１２Ａ、１２Ｂ、１２Ｃ、１２Ｄ、・・・を備える。公証装置１１および端末１２Ａ、１２Ｂ、１２Ｃ、１２Ｄ、・・・は、通信ネットワーク１３を介して互いに結合されている。

【００２７】図４は、公証装置１１およびユーザ端末１２Ａ、１２Ｂ、１２Ｃ、１２Ｄとして用いられる情報処理装置の構成図である。図４の情報処理装置は、ＣＰＵ２１、メモリ２２、入力装置２３、出力装置２４、外部記憶装置２５、媒体駆動装置２６、ネットワーク接続装置２７を備え、それらの各装置はバス２８により互いに結合されている。

【００２８】ＣＰＵ２１は、メモリ２２を利用しながらプログラムを実行して、上述の各サービスを実現する。メモリ２２としては、例えばＲＯＭ（read only memory）、ＲＡＭ（random access memory）等が用いられる。メモリ２２には、上述のプログラムと、処理に必要なデータが格納される。

【００２９】入力装置２２は、例えばキーボード、ポインティングデバイス等に相当し、ユーザからの要求や指示の入力に用いられる。また、出力装置２４は、表示装置やプリンタ等に相当し、取り引き情報等の出力に用いられる。

【００３０】外部記憶装置２５は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。この外部記憶装置２５に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ２２にロードして使用することができる。また、外部記憶装置２５は、取り引き情報を保存するデータベースとしても使用される。

【００３１】媒体駆動装置２６は、可搬記録媒体２９を駆動し、その記憶内容にアクセスすることができる。可搬記録媒体２９としては、メモリカード、フロッピーディスク、ＣＤ－ＲＯＭ（compact disk read only memory）、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体を使用することができる。この可搬記録媒体２９に、上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ２２にロードして使用することができる。

【００３２】ネットワーク接続装置２７は、通信ネットワーク１３に接続され、通信に伴うデータ変換等を行う。情報処理装置は、ネットワーク接続装置２７を介して、取り引き情報等を送受信することができる。また、情報処理装置は、必要に応じて、外部の情報提供者のデータベース３０等と通信して、データベース３０から上述のプログラムとデータを受け取り、それらをメモリ２２にロードして使用することができる。

【００３３】ところで、上述のサービスのうち、身元保証サービスは、今日の社会における印鑑証明サービスに相当する。印鑑証明サービスは、取り引きの当事者の身元が確かなことを保証するサービスである。当事者は役所に印鑑を登録しておき、取り引き文書にその印鑑で朱印を押すことで自分の身元を証明する。

【００３４】このサービスをネットワーク上で実現するために、公証人Ｎが電子署名の正当性を証明する。電子署名とは、データの送信者が本人しか知らない秘密鍵を用いて、なんらかの方法でデータを暗号化して作成した情報である。この情報は、本人しか生成することができないので、ネットワーク環境では印鑑の印影と同様の役割を果たす。

11

【００３５】具体的には、ＩＴＵ（International Telecommunication Union）　Ｘ．５０９で勧告されている認証局の枠組を利用することができる。この枠組みによれば、当事者の身元が確かであることを確認するためには、認証局から発行される証明書の中の公開鍵を用いて電子署名を復号化し、その内容を検証すればよい。電子署名の生成に用いられる秘密鍵と証明書に記載される公開鍵とは対になっており、秘密鍵により暗号化されたデータは公開鍵により復号化することができる。

【００３６】また、公証人Ｎは、取り引きした日付けや時刻を表す日時情報を当事者に発行することで、日時保証サービスを提供する。これにより、取り引きした日時を保証し、同じ当事者間の過去の取り引き内容との混同を避けることができる。

【００３７】さらに、公証人Ｎは、取り引きの識別子としてトランザクションＩＤを当事者に発行することで、一意性保証サービスを提供する。これにより、各取り引きが正しく識別され、他の取り引き内容との混同を避けることができる。

【００３８】また、配達保証サービスは、ＩＳＯ（International Standardization Organization）／ＩＥＣ（International Electrotechnical Commission）　ＣＤ１３８８８－１，２，３により標準化されている否認拒否機構（non-repudiation mechanism）を用いて実現することができる。この否認拒否機構は、配達の証拠となるトークン情報を発行し、ユーザの要求に応じてそれを確認することで、メッセージが配達されたことを証明する。以下では、この配達保証サービスについては詳述を避けることにする。

【００３９】次に、図５から図１０までを参照しながら、内容保証サービスの実施形態について説明する。２人の当事者間でやりとりされる取り引き情報の内容を保証するには、以下のようなサービス要件が考えられる。

［１］取り引き内容を発信者が確認したことを保証するために、取り引き内容に発信者の電子署名を付加する。

［２］取り引き内容を受信者が確認したことを保証するために、取り引き内容に受信者の電子署名を付加する。

［３］最終的に発信者および受信者が取り引き内容を確認したことを保証するために、発信者および受信者の電子署名が付いた取り引き情報を、発信者、受信者、および公証人Ｎが共有する。

［４］取り引き内容をいつでも参照できることを保証するために、公証人Ｎが取り引き内容を蓄積する。

【００４０】以上の要件を満たすためには、発信者と受信者の電子署名が付いた取り引き情報を、発信者、受信者、および公証人Ｎが共有する必要がある。図５においては、取り引き内容が記述された取り引き文書Ｍと、それに対するユーザＡの電子署名ＳＡ（Ｍ）と、ユーザＢの電子署名ＳＢ（Ｍ）とが、ユーザＡ、Ｂ、および公証人Ｎにより共有されている。

12

【００４１】図６は、図５の取り引き文書Ｍの一例を示している。図６の取り引き文書Ｍの中には、売買の当事者、売買の対象、売買金額、売買日時等の取り引き内容を記述した平文Ｐのほかに、公証人Ｎが発行する日時情報Ｔとトランザクションが含まれている。ここでは、“１９９６０８０８１４２３５６”が日時情報Ｔに相当し、“１９９６年８月８日１４時２３分５６秒”を表している。また、“４５６７”は、トランザクションＩＤが“０ｘ４５６７（１６進数）”であることを表している。

【００４２】Ｎの電子署名ＳＮ（Ｔ，ＩＤ）は、日時情報Ｔとトランザクションを連結したデータに対する公証人Ｎの電子署名を表す。このＳＮ（Ｔ，ＩＤ）の代わりに、日時情報Ｔのみに対する公証人Ｎの電子署名ＳＮ（Ｔ）とトランザクションのみに対する公証人Ｎの電子署名ＳＮ（ＩＤ）を付加してもよい。

【００４３】このような内容保証サービスの実施形態としては、図７、８、９、１０に示すような４つの基本モデルが考えられる。これらのモデルにおいては、図６のような取り引き文書Ｍが用いられ、ユーザＡ、Ｂ、および公証人Ｎの間でやりとりされる情報には発信者の電子署名が付いている。受信者はその電子署名を検証することで、発信者の身元を確認することができる。したがって、これらのモデルは、身元保証サービス、日時保証サービス、および一意性保証サービスを含んでいる。

【００４４】図７は、内容保証サービスの第１のモデルを示している。第１のモデルでは、ユーザＡ、Ｂがオンラインまたはオフラインで取り引き内容Ｐを交換した後、それぞれが公証装置１１に対して取り引き情報を送付する。図７における処理の流れは、次のようになる。

【００４５】Ｐ０：ユーザＡの端末１２Ａが、公証装置１１から日時情報Ｔとトランザクションを取得する。

Ｐ０′：ユーザＢの端末１２Ｂが、公証装置１１から日時情報Ｔとトランザクションを取得する。

【００４６】処理Ｐ０およびＰ０′において、公証装置１１は、取り引きの当事者であるユーザＡとユーザＢに、同一の日時情報Ｔとトランザクションを発行する。

Ｐ１：端末１２Ａが、日時情報Ｔとトランザクションと取り引き内容Ｐを連結して、取り引き文書Ｍを作成する。次に、ユーザＡの秘密鍵ＳＡを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＡ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ）｝を公証装置１１に送信する。

【００４７】電子署名ＳＡ（Ｍ）の作成方法としては、任意のものを用いることができる。例えば、取り引き文書Ｍを所定の圧縮アルゴリズムで圧縮したり、ハッシュしたりしてデータ量を削減し、得られたデータを秘密鍵ＳＡで暗号化する方法がある。もちろん、取り引き文書

Ｍをそのまま秘密鍵ＳＡで暗号化してもかまわない。

【００４８】Ｐ１′：端末１２Ｂが、日時情報Ｔとトランザクション ＩＤと取り引き内容Ｐを連結して、取り引き文書Ｍ′を作成する。次に、ユーザＢの秘密鍵ＳＢを取り出し、それを用いて取り引き文書Ｍ′に対する電子署名ＳＢ（Ｍ′）を作成する。そして、データ｛Ｍ′，ＳＢ（Ｍ′）｝を公証装置１１に送信する。

【００４９】Ｐ２：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ）｝とデータ｛Ｍ′，ＳＢ（Ｍ′）｝を受信する。そして、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ′）を検証する。

【００５０】例えば、圧縮処理やハッシュ処理により、電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ′）の中の取り引き文書Ｍ、Ｍ′のデータ量が削減されている場合は、公証装置１１は、受け取った取り引き文書Ｍ、Ｍ′に同様のデータ削減処理を施す。そして、得られたデータと、ＳＡ（Ｍ）、ＳＢ（Ｍ′）を公開鍵ＰＡ、ＰＢで復号化したデータとを、それぞれ比較して、ＳＡ（Ｍ）、ＳＢ（Ｍ′）の正当性を検証する。

【００５１】もじ、圧縮処理やハッシュ処理が行われていない場合は、受け取った取り引き文書Ｍ、Ｍ′を、そのまま、ＳＡ（Ｍ）、ＳＢ（Ｍ′）を復号化したデータと比較するだけでよい。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ′）が正しくなければ、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【００５２】次に、公証装置１１は、取り引き文書ＭとＭ′が同一かどうかを確認する。具体的には、これらの取り引き文書に記述された日時情報Ｔ、トランザクション ＩＤ、取り引き内容Ｐをそれぞれ比較し、両者が一致することを確認する。また、取り引き文書Ｍの中の日時情報Ｔとトランザクション ＩＤが、発行したものと一致するかどうかを確認する。

【００５３】取り引き文書ＭとＭ′が一致しない場合、あるいは、日時情報ＴまたはトランザクションＩＤが正しくない場合は、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【００５４】次に、公証装置１１は、取り引き文書Ｍ、電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ′）を連結して、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝を作成し、それを保存する。

【００５５】Ｐ３：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝を端末１２Ａに送信する。

Ｐ３′：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝を端末１２Ｂに送信する。

【００５６】Ｐ４：端末１２Ａが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝を受信する。そして、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ′）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ′）が正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。

【００５７】次に、端末１２Ａは、公証装置１１から受け取った取り引き文書Ｍと端末１２Ａが作成した取り引き文書Ｍが同一かどうかを確認する。受け取った取り引き文書Ｍが正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。それが正しければ、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝を保存して、処理を終了する。

【００５８】Ｐ４′：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝を受信する。そして、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ′）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ′）が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。

【００５９】次に、端末１２Ｂは、公証装置１１から受け取った取り引き文書Ｍ′と端末１２Ｂが作成した取り引き文書Ｍ′が同一かどうかを確認する。受け取った取り引き文書Ｍ′が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。それが正しければ、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝を保存して、処理を終了する。

【００６０】このような第１のモデルでは、ユーザＡ、Ｂの双方が独立に取り引き情報を公証人Ｎに送付するため、ユーザＡとユーザＢが対等な立場にあるといえる。また、ユーザＡ、Ｂは、各自の電子署名を付けるだけでサービスを受けることができる。一方、公証装置１１は、ユーザＡ、Ｂの電子署名の検証の他に、取り引き文書ＭとＭ′の同一性の検証を行わなければならない。

【００６１】ただし、このモデルでは、公証装置１１が取り引き文書Ｍ、Ｍ′の同一性の検証に失敗した場合、ユーザＡ、Ｂのどちらが内容を改ざんしたのかを特定できない。また、ユーザＡとユーザＢの公証装置１１に対する取り引き情報の送付がタイミングよく行われず、公証装置１１がそれらを検証できない可能性もある。

【００６２】図８は、内容保証サービスの第２のモデルを示している。第２のモデルでは、ユーザＡ、Ｂがオンラインまたはオフラインで取り引き内容Ｐを交換した後、ユーザＡのみが公証装置１１に対して取り引き情報を送付する。図８における処理の流れは、次のようになる。

【００６３】Ｐ１０：ユーザＡの端末１２Ａが、公証装置１１から日時情報ＴとトランザクションＩＤを取得する。

Ｐ１１：端末１２Ａが、日時情報ＴとトランザクションＩＤと取り引き内容Ｐを連結して、取り引き文書Ｍを作成する。次に、ユーザＡの秘密鍵ＳＡを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＡ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ）｝を端末１

２Ｂに送信する。

【００６４】Ｐ１２：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ）｝を受信する。そして、ユーザＡの公開鍵ＰＡを取り出し、それを用いてＳＡ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。

【００６５】次に、ユーザＢの秘密鍵ＳＢを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＢ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を作成して、それを保存する。

【００６６】Ｐ１３：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を端末１２Ａに送信する。

Ｐ１４：端末１２Ａが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を受信する。そして、ユーザＢの公開鍵ＰＢを取り出し、それを用いてＳＢ（Ｍ）を検証する。ここで、ＳＢ（Ｍ）が正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。それが正しければ、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を保存する。

【００６７】Ｐ１５：端末１２Ａが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を公証装置１１に送信する。

Ｐ１６：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を受信する。そして、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ）が正しくなければ、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【００６８】次に、公証装置１１は、取り引き文書Ｍの中の日時情報Ｔとトランザクション ＩＤが、発行したものと一致するかどうかを確認する。日時情報Ｔまたはトランザクション ＩＤが正しくない場合は、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【００６９】電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ）、日時情報Ｔ、およびトランザクション ＩＤが正しければ、公証装置１１は、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を保存して、処理を終了する。

【００７０】このような第２のモデルでは、ユーザＡのみが取り引き情報を公証人Ｎに送付するため、最終的に内容保証サービスを受けるかどうかをユーザＡが決定することができる。したがって、ユーザＡの方が有利な立場にあるといえる。

【００７１】また、ユーザＢは、取り引き文書Ｍにユーザ Ａの電子署名が付いた情報がないとサービスを受けられない。一方、ユーザＡは、ユーザＢの電子署名がないとサービスを受けられないが、過去に作成されたユーザＢの電子署名付きの情報を公証人Ｎに送ることができる。

【００７２】図９は、内容保証サービスの第３のモデルを示している。第３のモデルでは、ユーザＡ、Ｂがオンラインまたはオフラインで取り引き内容Ｐを交換した後、ユーザＢのみが公証装置１１に対して取り引き情報を送付する。図９における処理の流れは、次のようになる。

【００７３】Ｐ２０：ユーザＡの端末１２Ａが、公証装置１１から日時情報Ｔとトランザクション ＩＤを取得する。

Ｐ２１：端末１２Ａが、日時情報Ｔとトランザクション ＩＤと取り引き内容Ｐを連結して、取り引き文書Ｍを作成する。次に、ユーザＡの秘密鍵ＳＡを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＡ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ）｝を端末１２Ｂに送信する。

【００７４】Ｐ２２：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ）｝を受信する。そして、ユーザＡの公開鍵ＰＡを取り出し、それを用いてＳＡ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。

【００７５】次に、ユーザＢの秘密鍵ＳＢを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＢ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を作成して、それを保存する。

【００７６】Ｐ２３：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を公証装置１１に送信する。

Ｐ２４：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を受信する。そして、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ）が正しくなければ、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【００７７】次に、公証装置１１は、取り引き文書Ｍの中の日時情報Ｔとトランザクション ＩＤが、発行したものと一致するかどうかを確認する。日時情報Ｔまたはトランザクション ＩＤが正しくない場合は、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【００７８】電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ）、日時情報Ｔ、およびトランザクション ＩＤが正しければ、公証装置１１は、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を保存する。

【００７９】Ｐ２５：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を端末１２Ａに送信する。

Ｐ２６：端末１２Ａが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を受信する。そして、ユーザＡ、Ｂ、の公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ）が正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。それらが正しければ、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を保存して、処理を終了する。

【００８０】このような第３のモデルでは、ユーザＢのみが取り引き情報を公証人Ｎに送付するため、最終的に

内容保証サービスを受けるかどうかをユーザＢが決定することができる。したがって、ユーザＢの方が有利な立場にあるといえる。しかし、ユーザＢは、取り引き文書Ｍにユーザの電子署名が付いた情報がないとサービスを受けられない。一方、ユーザＡは、公証人Ｎから取り引き情報を受け取らないと、ユーザＢが承認したのかどうかが分からない。

【００８１】図１０は、内容保証サービスの第４のモデルを示している。第４のモデルでは、公証装置１１がユーザＡとユーザＢの取り引きを仲介する。図１０における処理の流れは、次のようになる。

【００８２】Ｐ３０：ユーザＡの端末１２Ａが、公証装置１１から日時情報Ｔとトランザクション ＩＤを取得する。

Ｐ３１：端末１２Ａが、日時情報Ｔとトランザクション ＩＤと取り引き内容Ｐを連結して、取り引き文書Ｍを作成する。次に、ユーザＡの秘密鍵ＳＡを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＡ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ）｝を公証装置１１に送信する。

【００８３】Ｐ３２：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ）｝を受信する。そして、ユーザＡの公開鍵ＰＡを取り出し、それを用いてＳＡ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）が正しくなければ、端末１２Ａにエラー通知を行って処理を終了する。それが正しければ、データ｛Ｍ，ＳＡ（Ｍ）｝を端末１２Ｂに送信する。

【００８４】Ｐ３３：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ）｝を受信する。ユーザＢは、受け取った取り引き文書Ｍの中の取り引き内容Ｐを見て、その取り引きに応じられない場合は、その旨を端末１２Ａに通知し、端末１２Ｂの処理を終了させる。また、その取り引きに応じる場合は、端末１２Ｂに処理の続行を指示する。

【００８５】次に、端末１２Ｂは、ユーザＡの公開鍵ＰＡを取り出し、それを用いてＳＡ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。

【００８６】次に、端末１２Ｂは、ユーザＢの秘密鍵ＳＢを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＢ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を作成して、それを保存する。

【００８７】Ｐ３４：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を公証装置１１に送信する。

Ｐ３５：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を受信する。そして、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ）が正しくなければ、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【００８８】次に、公証装置１１は、取り引き文書Ｍの中の日時情報Ｔとトランザクション ＩＤが、発行したものと一致するかどうかを確認する。日時情報Ｔまたはトランザクション ＩＤが正しくない場合は、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【００８９】電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ）、日時情報Ｔ、およびトランザクション ＩＤが正しければ、公証装置１１は、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を保存する。

【００９０】Ｐ３６：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を端末１２Ａに送信する。

Ｐ３７：端末１２Ａが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を受信する。そして、ユーザＡ、Ｂ、の公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ）が正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。それらが正しければ、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を保存して、処理を終了する。

【００９１】このような第４のモデルでは、ユーザＡとユーザＢの取り引きを公証人Ｎが仲介するため、取り引き内容の改ざんが行われた場合、ユーザＡとユーザＢのどちらが改ざんしたかを公証人Ｎが特定することができる。

【００９２】以上説明したモデルのうち、第２および第３のモデルでは、ユーザＡとユーザＢの間で取り引き情報がやりとりされるので、送信者の電子署名を検証するために公開鍵を用いる必要がある。したがって、ＲＳＡ（Rivest-Shamir-Adleman）暗号のような公開鍵システムが前提となる。

【００９３】これに対して、第１および第４のモデルでは、ユーザＡと公証人Ｎの間またはユーザＢと公証人Ｎの間で取り引き情報がやりとりされ、ユーザＡとユーザＢの間では取り引き情報がやりとりされない。この場合、ＤＥＳ（Data EncryptionStandard）暗号のような秘密鍵システムでも、身元保証サービスを実現することが可能である。ただし、公証人Ｎはユーザ Ａとユーザ Ｂの秘密鍵を知っている必要がある。

【００９４】次に、図１１から図１９までを参照しながら、取り引き保証サービスの実施形態について説明する。ユーザＡとユーザＢが取り引きした事実を保証するには、以下のようなサービス要件が考えられる。

〈１〉ユーザＢと取り引きした事実をユーザＡが第３者Ｃに対して証明するために、取り引き文書にユーザＢの電子署名を付けた情報に対して、公証人Ｎの電子署名を付ける。

〈２〉ユーザＡと取り引きした事実をユーザＢが第３者Ｃに対して証明するために、取り引き文書にユーザＡの電子署名を付けた情報に対して、公証人Ｎの電子署名を付ける。

〈３〉ユーザＢと取り引きした事実をユーザＡが否定できないように、取り引き文書にユーザＡの電子署名を付

けた情報に対する公証人Ｎの電子署名を、公証人Ｎとユーザ Ｂが保持する。

〈４〉ユーザＡと取り引きした事実をユーザＢが否定できないように、取り引き文書にユーザＢの電子署名を付けた情報に対する公証人Ｎの電子署名を、公証人Ｎとユーザ Ａが保持する。

【００９５】以上の要件を満たすためには、取り引き文書にユーザＡとユーザＢの電子署名を付けた情報に対する公証人Ｎの電子署名を、最終的にユーザＡ、Ｂ、および公証人Ｎが共有すればよい。図１１においては、取り引き文書Ｍ、ユーザＡの電子署名ＳＡ（Ｍ）、およびユーザＢの電子署名ＳＢ（Ｍ）を連結した情報に対する公証人Ｎの電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））が、ユーザＡ、Ｂ、および公証人Ｎにより共有されている。

【００９６】この取り引き保証サービスは、上述の内容保証サービスと密接に関係しているため、内容保証サービスの実施形態を元にして実現される。図７、８、９、１０に示した４つの基本モデルに対応して、取り引き保証サービスの基本モデルは、図１２、１３、１４、１５に示す４つのモデルになる。

【００９７】これらのモデルにおいては、内容保証サービスと同様に、図６のような取り引き文書Ｍが用いられ、ユーザＡ、Ｂ、および公証人Ｎの間でやりとりされる情報には発信者の電子署名が付いている。受信者はその電子署名を検証することで、発信者の身元を確認することができる。したがって、これらのモデルは、身元保証サービス、日時保証サービス、一意性保証サービス、および内容保証サービスを含んでいる。

【００９８】図１２は、取り引き保証サービスの第１のモデルを示している。第１のモデルでは、ユーザＡ、Ｂがオンラインまたはオフラインで取り引き内容Ｐを交換した後、それぞれが公証装置１１に対して取り引き情報を送付する。図１２における処理の流れは、次のようになる。

【００９９】Ｐ４０：ユーザＡの端末１２Ａが、公証装置１１から日時情報Ｔとトランザクション ＩＤを取得する。

Ｐ４０′：ユーザＢの端末１２Ｂが、公証装置１１から日時情報Ｔとトランザクション ＩＤを取得する。

【０１００】Ｐ４１：端末１２Ａが、日時情報Ｔとトランザクション ＩＤと取り引き内容Ｐを連結して、取り引き文書Ｍを作成する。次に、ユーザＡの秘密鍵ＳＡを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＡ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ）｝を公証装置１１に送信する。

【０１０１】Ｐ４１′：端末１２Ｂが、日時情報Ｔとトランザクション ＩＤと取り引き内容Ｐを連結して、取り引き文書Ｍ′を作成する。次に、ユーザＢの秘密鍵ＳＢを取り出し、それを用いて取り引き文書Ｍ′に対する電子署名ＳＢ（Ｍ′）を作成する。そして、データ｛Ｍ′，ＳＢ（Ｍ′）｝を公証装置１１に送信する。

【０１０２】Ｐ４２：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ）｝とデータ｛Ｍ′，ＳＢ（Ｍ′）｝を受信する。そして、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ′）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ′）が正しくなければ、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【０１０３】次に、公証装置１１は、取り引き文書ＭとＭ′が同一かどうかを確認する。また、取り引き文書Ｍの中の日時情報Ｔとトランザクション ＩＤが、発行したものと一致するかどうかを確認する。取り引き文書ＭとＭ′が一致しない場合、あるいは、日時情報Ｔまたはトランザクション ＩＤが正しくない場合は、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【０１０４】次に、公証装置１１は、取り引き文書Ｍ、電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ′）を連結して、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝を作成する。次に、公証人Ｎの秘密鍵ＳＮを取り出し、それを用いてデータ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝に対する電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））｝を保存する。

【０１０５】Ｐ４３：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））｝を端末１２Ａに送信する。

Ｐ４３′：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））｝を端末１２Ｂに送信する。

【０１０６】Ｐ４４：端末１２Ａが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））｝を受信する。そして、公証人Ｎの公開鍵ＰＮを取り出し、それを用いて電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））を検証する。また、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ′）を検証する。ここで、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））、ＳＡ（Ｍ）、ＳＢ（Ｍ′）のいずれかが正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。

【０１０７】次に、端末１２Ａは、公証装置１１から受け取った取り引き文書Ｍと端末１２Ａが作成した取り引き文書Ｍが同一かどうかを確認する。受け取った取り引き文書Ｍが正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。それが正しければ、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））｝を保存して、処理を終了する。

【０１０８】Ｐ４４′：端末１２Ｂが、データ｛Ｍ，Ｓ

Ａ（Ｍ），ＳＢ（Ｍ′），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））｝を受信する。そして、公証人Ｎの公開鍵ＰＮを取り出し、それを用いて電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））を検証する。また、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ′）を検証する。ここで、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））、ＳＡ（Ｍ）、ＳＢ（Ｍ′）のいずれかが正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。

【０１０９】次に、端末１２Ｂは、公証装置１１から受け取った取り引き文書Ｍ′と端末１２Ｂが作成した取り引き文書Ｍ′が同一かどうかを確認する。受け取った取り引き文書Ｍ′が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。それが正しければ、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））｝を保存して、処理を終了する。

【０１１０】図１３は、取り引き保証サービスの第２のモデルを示している。第２のモデルでは、ユーザＡ、Ｂがオンラインまたはオフラインで取り引き内容Ｐを交換した後、ユーザＡのみが公証装置１１に対して取り引き情報を送付する。図１３における処理の流れは、次のようになる。

【０１１１】Ｐ５０：ユーザＡの端末１２Ａが、公証装置１１から日時情報Ｔとトランザクション ＩＤを取得する。

Ｐ５１：端末１２Ａが、日時情報Ｔとトランザクション ＩＤと取り引き内容Ｐを連結して、取り引き文書Ｍを作成する。次に、ユーザＡの秘密鍵ＳＡを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＡ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ）｝を端末１２Ｂに送信する。

【０１１２】Ｐ５２：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ）｝を受信する。そして、ユーザＡの公開鍵ＰＡを取り出し、それを用いてＳＡ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。

【０１１３】次に、ユーザＢの秘密鍵ＳＢを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＢ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を作成して、それを保存する。

【０１１４】Ｐ５３：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を端末１２Ａに送信する。

Ｐ５４：端末１２Ａが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を受信する。そして、ユーザＢの公開鍵ＰＢを取り出し、それを用いてＳＢ（Ｍ）を検証する。ここで、ＳＢ（Ｍ）が正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。それが正しければ、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を保存する。

【０１１５】Ｐ５５：端末１２Ａが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を公証装置１１に送信する。

Ｐ５６：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を受信する。そして、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ）が正しくなければ、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【０１１６】次に、公証装置１１は、取り引き文書Ｍの中の日時情報Ｔとトランザクション ＩＤが、発行したものと一致するかどうかを確認する。日時情報Ｔまたはトランザクション ＩＤが正しくない場合は、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【０１１７】次に、公証装置１１は、公証人Ｎの秘密鍵ＳＮを取り出し、それを用いてデータ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝に対する電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））｝を作成し、それを保存する。

【０１１８】Ｐ５７：公証装置１１が、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を端末１２Ａに送信する。

Ｐ５７′：公証装置１１が、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を端末１２Ｂに送信する。

【０１１９】Ｐ５８：端末１２Ａが、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を受信する。そして、公証人Ｎの公開鍵ＰＮを取り出し、それを用いてＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を検証する。ここで、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））が正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。それが正しければ、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を保存して、処理を終了する。

【０１２０】Ｐ５８′：端末１２Ｂが、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を受信する。そして、公証人Ｎの公開鍵ＰＮを取り出し、それを用いてＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を検証する。ここで、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。それが正しければ、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を保存して、処理を終了する。

【０１２１】図１４は、取り引き保証サービスの第３のモデルを示している。第３のモデルでは、ユーザＡ、Ｂがオンラインまたはオフラインで取り引き内容Ｐを交換した後、ユーザＢのみが公証装置１１に対して取り引き情報を送付する。図１４における処理の流れは、次のようになる。

【０１２２】Ｐ６０：ユーザＡの端末１２Ａが、公証装

置１１から日時情報Ｔとトランザクション ＩＤを取得する。

Ｐ６１：端末１２Ａが、日時情報Ｔとトランザクション ＩＤと取り引き内容Ｐを連結して、取り引き文書Ｍを作成する。次に、ユーザＡの秘密鍵ＳＡを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＡ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ）｝を端末１２Ｂに送信する。

【０１２３】Ｐ６２：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ）｝を受信する。そして、ユーザＡの公開鍵ＰＡを取り出し、それを用いてＳＡ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。

【０１２４】次に、ユーザＢの秘密鍵ＳＢを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＢ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を作成して、それを保存する。

【０１２５】Ｐ６３：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を公証装置１１に送信する。

Ｐ６４：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を受信する。そして、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ）が正しくなければ、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【０１２６】次に、公証装置１１は、取り引き文書Ｍの中の日時情報Ｔとトランザクション ＩＤが、発行したものと一致するかどうかを確認する。日時情報Ｔまたはトランザクション ＩＤが正しくない場合は、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【０１２７】次に、公証装置１１は、公証人Ｎの秘密鍵ＳＮを取り出し、それを用いてデータ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝に対する電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））｝を作成し、それを保存する。

【０１２８】Ｐ６５：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））｝を端末１２Ａに送信する。

Ｐ６５′：公証装置１１が、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を端末１２Ｂに送信する。

【０１２９】Ｐ６６：端末１２Ａが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））｝を受信する。そして、ユーザＡ、Ｂ、公証人Ｎの公開鍵ＰＡ、ＰＢ、ＰＮを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ）を検証し、公開鍵ＰＮでＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を検証する。

【０１３０】ここで、ＳＡ（Ｍ）、ＳＢ（Ｍ）、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））のいずれかが正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。それらが正しければ、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））｝を保存して、処理を終了する。

【０１３１】Ｐ６６′：端末１２Ｂが、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を受信する。そして、公証人Ｎの公開鍵ＰＮを取り出し、それを用いてＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を検証する。ここで、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。それが正しければ、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を保存して、処理を終了する。

【０１３２】図１５は、取り引き保証サービスの第４のモデルを示している。第４のモデルでは、公証装置１１がユーザＡとユーザＢの取り引きを仲介する。図１５における処理の流れは、次のようになる。

【０１３３】Ｐ７０：ユーザＡの端末１２Ａが、公証装置１１から日時情報Ｔとトランザクション ＩＤを取得する。

Ｐ７１：端末１２Ａが、日時情報Ｔとトランザクション ＩＤと取り引き内容Ｐを連結して、取り引き文書Ｍを作成する。次に、ユーザＡの秘密鍵ＳＡを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＡ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ）｝を公証装置１１に送信する。

【０１３４】Ｐ７２：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ）｝を受信する。そして、ユーザＡの公開鍵ＰＡを取り出し、それを用いてＳＡ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）が正しくなければ、端末１２Ａにエラー通知を行って処理を終了する。それが正しければ、データ｛Ｍ，ＳＡ（Ｍ）｝を端末１２Ｂに送信する。

【０１３５】Ｐ７３：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ）｝を受信する。ユーザＢは、受け取った取り引き文書Ｍの中の取り引き内容Ｐを見て、その取り引きに応じられない場合は、その旨を端末１２Ａに通知し、端末１２Ｂの処理を終了させる。また、その取り引きに応じる場合は、端末１２Ｂに処理の続行を指示する。

【０１３６】次に、端末１２Ｂは、ユーザＡの公開鍵ＰＡを取り出し、それを用いてＳＡ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。

【０１３７】次に、端末１２Ｂは、ユーザＢの秘密鍵ＳＢを取り出し、それを用いて取り引き文書Ｍに対する電子署名ＳＢ（Ｍ）を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を作成して、それを保存する。

【０１３８】Ｐ７４：端末１２Ｂが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を公証装置１１に送信する。

Ｐ７５：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝を受信する。そして、ユーザＡ、Ｂの公開鍵

ＰＡ、ＰＢを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ）を検証する。ここで、ＳＡ（Ｍ）またはＳＢ（Ｍ）が正しくなければ、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【０１３９】次に、公証装置１１は、取り引き文書Ｍの中の日時情報Ｔとトランザクション ＩＤが、発行したものと一致するかどうかを確認する。日時情報Ｔまたはトランザクション ＩＤが正しくない場合は、端末１２Ａ、１２Ｂにエラー通知を行って処理を終了する。

【０１４０】次に、公証装置１１は、公証人Ｎの秘密鍵ＳＮを取り出し、それを用いてデータ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ）｝に対する電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を作成する。そして、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））｝を作成し、それを保存する。

【０１４１】Ｐ７６：公証装置１１が、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））｝を端末１２Ａに送信する。

Ｐ７６′：公証装置１１が、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を端末１２Ｂに送信する。

【０１４２】Ｐ７７：端末１２Ａが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））｝を受信する。そして、ユーザＡ、Ｂ、公証人Ｎの公開鍵ＰＡ、ＰＢ、ＰＮを取り出し、公開鍵ＰＡでＳＡ（Ｍ）を検証し、公開鍵ＰＢでＳＢ（Ｍ）を検証し、公開鍵ＰＮでＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を検証する。

【０１４３】ここで、ＳＡ（Ｍ）、ＳＢ（Ｍ）、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））のいずれかが正しくなければ、公証装置１１、端末１２Ｂにエラー通知を行って処理を終了する。それらが正しければ、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ），ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））｝を保存して、処理を終了する。

【０１４４】Ｐ７７′：端末１２Ｂが、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を受信する。そして、公証人Ｎの公開鍵ＰＮを取り出し、それを用いてＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を検証する。ここで、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））が正しくなければ、公証装置１１、端末１２Ａにエラー通知を行って処理を終了する。それが正しければ、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ））を保存して、処理を終了する。

【０１４５】次に、図１６から図１９までのフローチャートを参照しながら、図１２に示した取り引き保証サービスの第１のモデルにおける公証装置１１、端末１２Ａ、１２Ｂの処理について、再び説明する。

【０１４６】図１６は、端末１２Ａの処理Ｐ４０、Ｐ４１、または端末１２Ｂの処理Ｐ４０′、Ｐ４１′に対応するフローチャートである。図１６において処理が開始されると、端末１２Ａ（または端末１２Ｂ）は、まず公

証装置１１からネットワーク１３を介して、日時情報Ｔとトランザクション ＩＤを取得する（ステップＳ１）。

【０１４７】次に、日時情報Ｔとトランザクション ＩＤと取り引き内容Ｐを連結して、図６のような取り引き文書Ｍ（またはＭ′）を作成する（ステップＳ２）。次に、ユーザの秘密鍵ＳＡ（またはＳＢ）を取り出し（ステップＳ３）、それを用いて取り引き文書Ｍに対するユーザの電子署名ＳＡ（Ｍ）（またはＳＢ（Ｍ′））を作成する（ステップＳ４）。

【０１４８】そして、取り引き文書Ｍ（またはＭ′）とユーザの電子署名ＳＡ（Ｍ）（またはＳＢ（Ｍ′））を、ネットワーク１３を介して公証装置１１に送信し（ステップＳ５）、処理を終了する。

【０１４９】図１７、１８は、公証装置１１の処理Ｐ４２、Ｐ４３、Ｐ４３′に対応するフローチャートである。図１７において処理が開始されると、公証装置１１は、まずネットワーク１３を介して、ユーザＡの端末１２Ａから取り引き文書Ｍと電子署名ＳＡ（Ｍ）を受信し、ユーザＢの端末１２Ｂから取り引き文書Ｍ′と電子署名ＳＢ（Ｍ′）を受信する（ステップＳ１１）。

【０１５０】次に、ユーザＡ、Ｂの公開鍵ＰＡ、ＰＢを取り出し（ステップＳ１２）、公開鍵ＰＡでＳＡ（Ｍ）を検証して（ステップＳ１３）、ＳＡ（Ｍ）が有効かどうかを判定する（ステップＳ１４）。ここでは、電子署名ＳＡ（Ｍ）を公開鍵ＰＡで復号化したデータが取り引き文書Ｍと同一とみなされるとき、ＳＡ（Ｍ）が有効となる。もし、ＳＡ（Ｍ）が有効でなければ、端末１２Ａ、１２Ｂにエラー通知を行って（ステップＳ１９）、処理を終了する。

【０１５１】ＳＡ（Ｍ）が有効であれば、次に、公開鍵ＰＢでＳＢ（Ｍ′）を検証して（ステップＳ１５）、ＳＢ（Ｍ′）が有効かどうかを判定する（ステップＳ１６）。ここで、ＳＢ（Ｍ′）が有効でなければ、端末１２Ａ、１２Ｂにエラー通知を行って（ステップＳ１９）、処理を終了する。

【０１５２】ＳＢ（Ｍ′）が有効であれば、次に、取り引き文書ＭとＭ′が一致するかどうかを確認する（ステップＳ１７）。これらが一致しなければ、端末１２Ａ、１２Ｂにエラー通知を行って（ステップＳ１９）、処理を終了する。

【０１５３】取り引き文書ＭとＭ′が一致すれば、次に、取り引き文書Ｍの中の日時情報Ｔとトランザクション ＩＤが、発行したものと一致するかどうかを確認する（ステップＳ１８）。日時情報Ｔまたはトランザクション ＩＤが正しくなければ、端末１２Ａ、１２Ｂにエラー通知を行って（ステップＳ１９）、処理を終了する。

【０１５４】これらが正しければ、次に、取り引き文書Ｍ、電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ′）を連結して、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝を作成する（図１８、ステップＳ２０）。

【０１５５】次に、公証人Ｎの秘密鍵ＳＮを取り出し（ステップＳ２１）、それを用いてデータ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝に対する公証人Ｎの電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））を作成する（ステップＳ２２）。そして、取り引き文書Ｍ、電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ′）、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））を保存する（ステップＳ２３）。

【０１５６】そして、これらのデータＭ、ＳＡ（Ｍ）、ＳＢ（Ｍ′）、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））を、ネットワーク１３を介して端末１２Ａ、１２Ｂに送信して（ステップＳ２４）、処理を終了する。

【０１５７】図１９は、端末１２Ａの処理Ｐ４４、または端末１２Ｂの処理Ｐ４４′に対応するフローチャートである。図１９において処理が開始されると、端末１２Ａ（または端末１２Ｂ）は、まずネットワーク１３を介して、公証装置１１から取り引き文書Ｍ、電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ′）、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））を受信する（ステップＳ３１）。

【０１５８】次に、公証人Ｎの公開鍵ＰＮを取り出し（ステップＳ３２）、それを用いて公証人Ｎの電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））を検証して（ステップＳ３３）、それが有効かどうかを判定する（ステップＳ３４）。ここでは、電子署名ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））を公開鍵ＰＮで復号化したデータが、データ｛Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′）｝と同一とみなされるとき、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））が有効となる。

【０１５９】もし、公証人Ｎの電子署名が有効でなければ、公証装置１１、端末１２Ｂ（または端末１２Ａ）にエラー通知を行って（ステップＳ４３）、処理を終了する。公証人Ｎの電子署名が有効であれば、次に、取り引き相手であるユーザＢ（またはユーザＡ）の公開鍵ＰＢ（またはＰＡ）を取り出し（ステップＳ３５）、それを用いて相手の電子署名ＳＢ（Ｍ′）（またはＳＡ（Ｍ））を検証して（ステップＳ３６）、それが有効かどうかを判定する（ステップＳ３７）。相手の電子署名が有効でなければ、公証装置１１、端末１２Ｂ（または端末１２Ａ）にエラー通知を行って（ステップＳ４３）、処理を終了する。

【０１６０】相手の電子署名が有効であれば、次に、当方の公開鍵ＰＡ（またはＰＢ）を取り出し（ステップＳ３８）、それを用いて当方の電子署名ＳＡ（Ｍ）（またはＳＢ（Ｍ′））を検証して（ステップＳ３９）、それが有効かどうかを判定する（ステップＳ４０）。当方の電子署名が有効でなければ、公証装置１１、端末１２Ｂ（または端末１２Ａ）にエラー通知を行って（ステップＳ４３）、処理を終了する。

【０１６１】当方の電子署名が有効であれば、次に、公証装置１１から受け取った取り引き文書Ｍが正しいかどうかを確認する（ステップＳ４１）。ここでは、受け取った取り引き文書Ｍが、当方が作成した取り引き文書Ｍ（またはＭ′）と同一であれば、それが正しいと判定する。受け取った取り引き文書Ｍが正しくなければ、公証装置１１、端末１２Ｂ（または端末１２Ａ）にエラー通知を行って（ステップＳ４３）、処理を終了する。

【０１６２】受け取った取り引き文書Ｍが正しければ、取り引き文書Ｍ、電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ′）、ＳＮ（Ｍ，ＳＡ（Ｍ），ＳＢ（Ｍ′））を保存して（ステップＳ４２）、処理を終了する。

【０１６３】こうして、図１６、１７、１８、１９に示した一連の処理により、取り引き文書、ユーザＡの電子署名、ユーザＢの電子署名、および公証人Ｎの電子署名が、ユーザＡ、Ｂ、公証人Ｎの間で共有されることになる。取り引き保証サービスの他のモデル、および内容保証サービスについても、同様のフローチャートを作成することが可能である。

【０１６４】公証装置１１は、取り引き内容を確認したい任意のユーザの端末から取り引き情報の参照要求を受け取ると、保存されている取り引き文書を、公証人Ｎの電子署名とともに要求元の端末に送り返す。こうして、要求者は、公証人Ｎにより保証された取り引き文書の内容を参照することができる。

【０１６５】以上、取り引き公証システムにおけるサービスとして、身元保証サービス、日時保証サービス、一意性保証サービス、配達保証サービス、内容保証サービス、および取り引き保証サービスについて述べたが、取り引き公証システムの望ましい実施形態は、図１２から図１５に示した４つの基本モデルから成ると考えられる。また、これらを元にした取り引き公証システムの応用モデルとして、暗号化モデル、多重署名モデル、および双方向モデルがある。

【０１６６】暗号化モデルとは、各基本モデルにおいてネットワーク上でやりとりされる情報全体を、受信者の公開鍵で暗号化して送信する実施形態である。受信者は、自分の秘密鍵で情報を復号化した後に、基本モデルと同様の処理を行う。このように情報を暗号化することで、ユーザＡ、Ｂと公証人Ｎ以外の者に取り引き情報を盗用される可能性が低くなる。

【０１６７】また、基本モデルでは、ユーザＡ、Ｂが、取り引き文書Ｍを元に電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ）を作成していた。多重署名モデルでは、取り引き文書Ｍと一方のユーザの電子署名とを連結した情報を元にして、もう一方のユーザが電子署名を作成する。例えば、ユーザＡが先に電子署名ＳＡ（Ｍ）を作成した場合、ユーザＢは、取り引き文書Ｍと電子署名ＳＡ（Ｍ）に対する電子署名ＳＢ（Ｍ，ＳＡ（Ｍ））を作成する。公証人Ｎは、さらに電子署名ＳＢ（Ｍ，ＳＡ（Ｍ））と取り引き文書Ｍを連結して、電子署名ＳＮ（ＳＢ（Ｍ，ＳＡ（Ｍ））を作成することになる。

【０１６８】この多重署名モデルによれば、ユーザＡ、

Ｂのどちらが先に取り引き文書Ｍを承認したのかを明らかにすることができる。また、この多重署名モデルで作成された情報を受信者の公開鍵で暗号化した暗号化モデルも考えられる。

【０１６９】また、図１３、１４、１５に示した第２、第３、第４のモデルでは、ユーザＡが取り引き文書Ｍの第１発信者であり、ユーザＢは受信した取り引き文書Ｍに基づいて応答するだけであった。

【０１７０】双方向モデルでは、これらの基本モデルにおいて、図１２に示した第１のモデルと同様に、ユーザＢからも取り引き文書Ｍ′を発信する。このように情報の流れを双方向にすることで、ユーザＡとユーザＢの立場が対等になる。この場合、公証装置１１は、双方からの情報を検証して登録することになる。

【０１７１】４つの基本モデルとそれらから派生する応用モデルを列挙すると、取り引き公証システムのモデルのバリエーションは、図２０に示すようになる。図２０において、例えば“多重署名＋暗号化”は、多重署名モデルと暗号化モデルを併用した複合モデルを表す。また、“○”は、対応する列の基本モデルと対応する行（第１行を除く）の応用モデルとの組合せが可能であることを表し、“×”は、その組合せが不可能であることを表す。

【０１７２】図２０から分かるように、取り引き公証システムには２３個のモデルがあることになる。さらに、取り引き公証システムの変形モデルとして、内容非開示モデルと合意署名モデルがある。

【０１７３】内容非開示モデルとは、公証人Ｎに取り引き内容を開示しないで、それを登録するモデルである。具体的には、各基本モデルおよび応用モデルにおいて、公証装置１１への送信情報から、取り引き内容の平文Ｐを削除することで実現される。この場合でも、ユーザＡ、Ｂの作成した電子署名は公証装置１１に送付されるので、公証装置１１はこれを検証／登録することができる。

【０１７４】また、合意署名モデルとは、保存する取り引き情報にユーザＡ、Ｂ、公証人Ｎ以外の合意者の電子署名を添付するモデルである。このモデルを採用することで、取り引きの当事者以外のユーザが、その取り引きの事実や内容に承認を与えたことを証明することが可能になる。

【０１７５】図２１は、このような合意署名を付加した共有情報の一例を示している。図２１においては、取り引き文書Ｍに対して、ユーザＡ、Ｂの電子署名ＳＡ（Ｍ）、ＳＢ（Ｍ）以外に、合意者であるユーザＣ、Ｄ、・・・の電子署名ＳＣ（Ｍ）、ＳＤ（Ｍ）、・・・も付加され、それらを連結した情報を元に公証人Ｎの電子署名ＳＮ（ＳＡ（Ｍ），ＳＢ（Ｍ），ＳＣ（Ｍ），ＳＤ（Ｍ），・・・）が作成されている。

【０１７６】このような合意署名モデルにおいて、ユーザＣ、Ｄ等が取り引きの当事者である場合は、取り引き公証システムは、自動的に３以上の当事者間の取り引きに関する事項を証明することになる。

【０１７７】

【発明の効果】本発明によれば、複数の情報処理装置を互いに接続したネットワーク環境において、ユーザ間で行われる取り引きの内容、日時、取り引き相手の身元等の取り引きに関する事項を、第３者が客観的に証明することができる。したがって、ネットワーク環境における取り引きの安全性が自動的に保証される。

【図面の簡単な説明】

【図１】本発明の原理図である。

【図２】ネットワーク上での商取り引き環境を示す図である。

【図３】取り引き公証システムを示す図である。

【図４】情報処理装置の構成図である。

【図５】内容保証サービスにおける共有情報を示す図である。

【図６】取り引き文書の例を示す図である。

【図７】第１の内容保証サービスを示す図である。

【図８】第２の内容保証サービスを示す図である。

【図９】第３の内容保証サービスを示す図である。

【図１０】第４の内容保証サービスを示す図である。

【図１１】取り引き保証サービスにおける共有情報を示す図である。

【図１２】第１の取り引き保証サービスを示す図である。

【図１３】第２の取り引き保証サービスを示す図である。

【図１４】第３の取り引き保証サービスを示す図である。

【図１５】第４の取り引き保証サービスを示す図である。

【図１６】ユーザ端末の第１の処理のフローチャートである。

【図１７】公証装置の処理のフローチャート（その１）である。

【図１８】公証装置の処理のフローチャート（その２）である。

【図１９】ユーザ端末の第２の処理のフローチャートである。

【図２０】取り引き公証システムのモデルを示す図である。

【図２１】合意署名を付加した共有情報を示す図である。

【符号の説明】

１　取り引き証明装置

２、３、１２Ａ、１２Ｂ、１２Ｃ、１２Ｄ　ユーザの端末装置

４、１３　通信ネットワーク

31

５　通信手段
６　処理手段
７　記憶手段
８、９　ユーザの電子署名データ
１１　公証装置
２１　ＣＰＵ
２２　メモリ
２３　入力装置

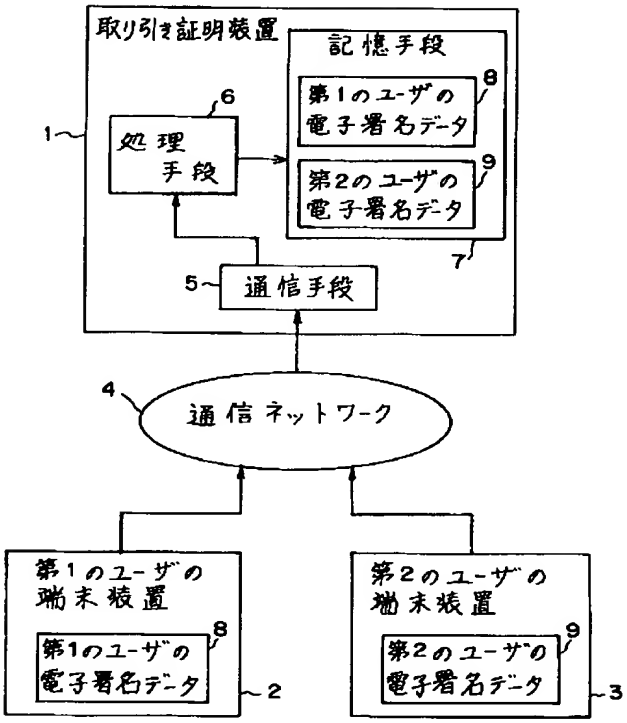
32

＊２４　出力装置
２５　外部記憶装置
２６　媒体駆動装置
２７　ネットワーク接続装置
２８　バス
２９　可搬記録媒体
３０　データベース

＊

【図１】

本発明の原理図



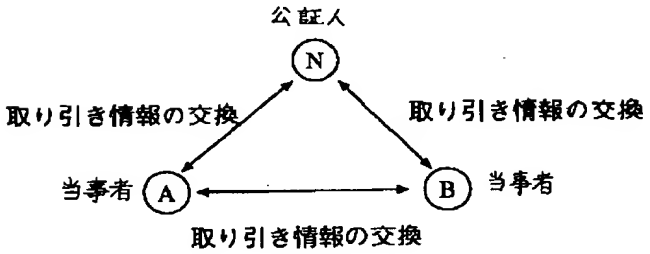
【図２０】

取り引き公証システムのモデルを示す図

	第1のモデル	第2のモデル	第3のモデル	第4のモデル
基本	○	○	○	○
暗号化	○	○	○	○
多重署名	×	○	○	○
多重署名＋暗号化	×	○	○	○
双方向	×	○	○	○
双方向＋暗号化	×	○	○	○
双方向＋暗号化＋多重署名	×	○	○	○

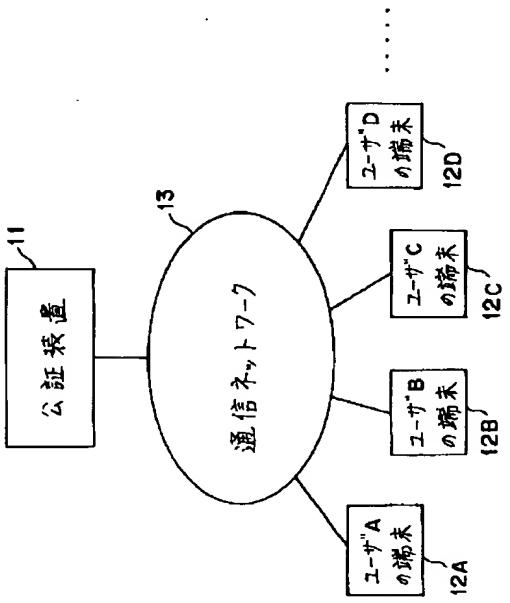
【図２】

ネットワーク上での商取り引き環境を示す図



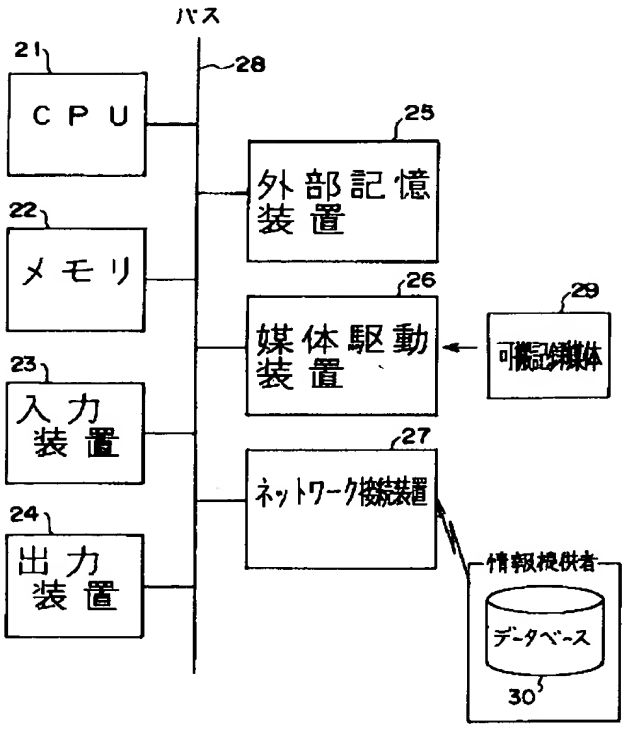
【図３】

取り引き公証システムを示す図



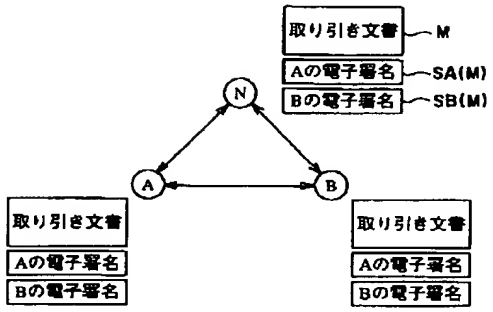
【図４】

情報処理装置の構成図



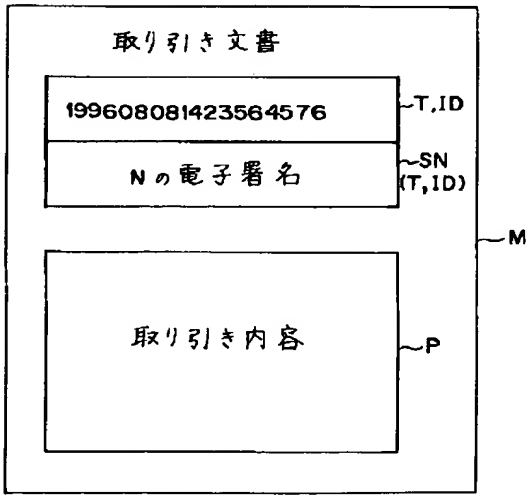
【図５】

内容保証サービスにおける共有情報を示す図



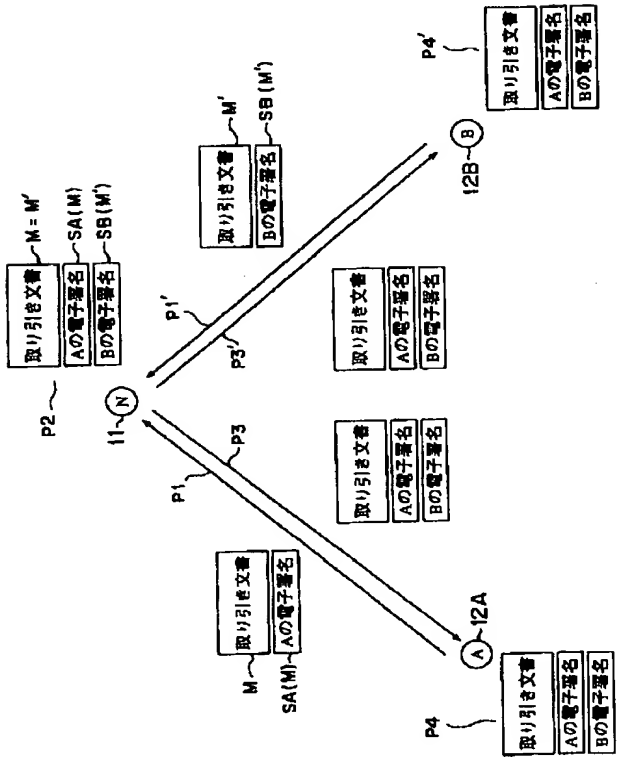
【図６】

取り引き文書の例を示す図



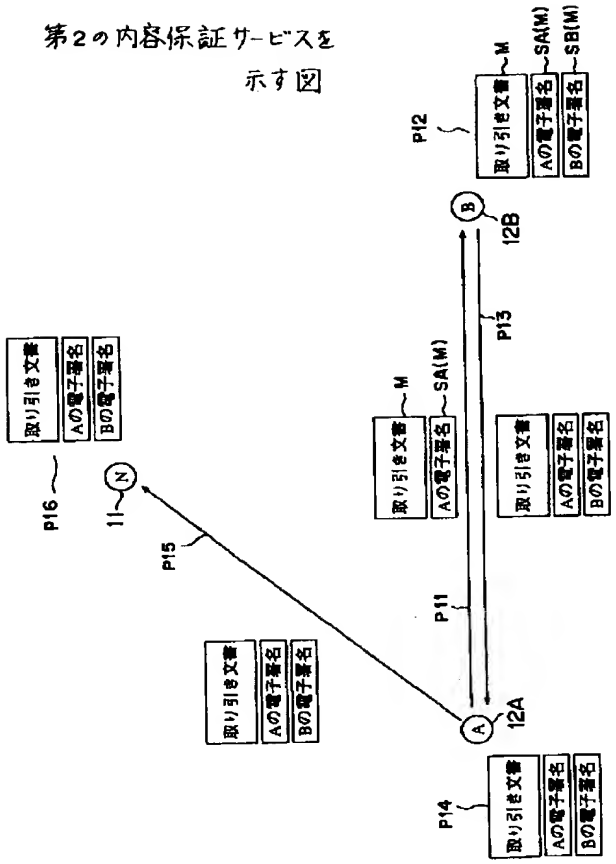
【図７】

第1の内容保証サービスを示す図



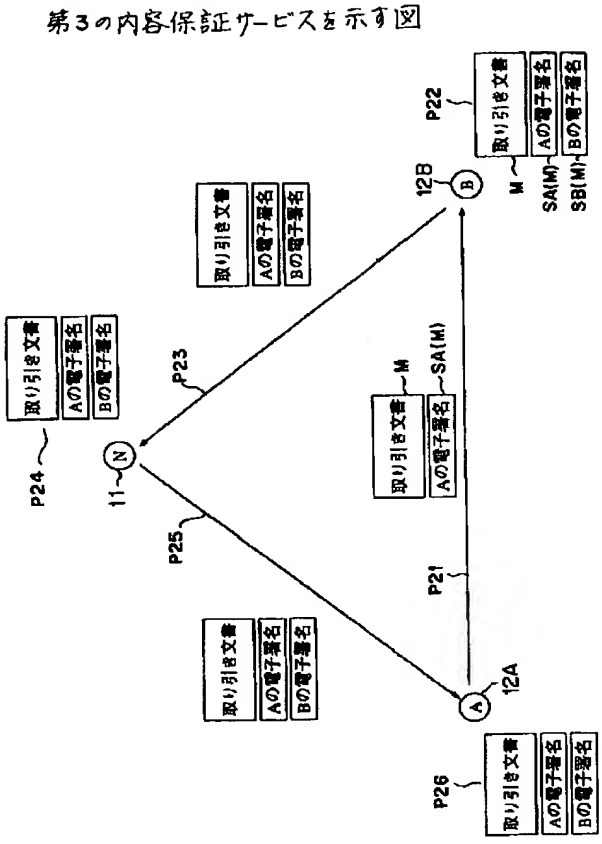
【図８】

第２の内容保証サービスを示す図



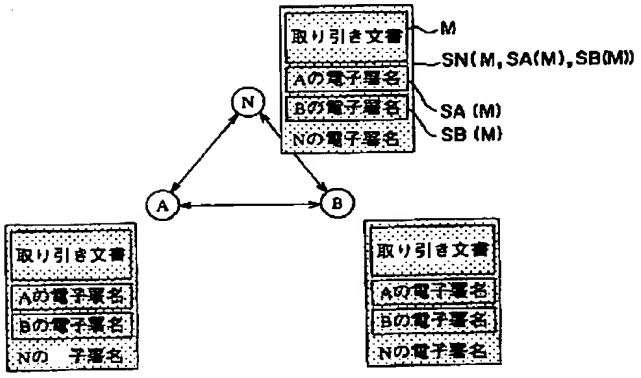
【図９】

第３の内容保証サービスを示す図



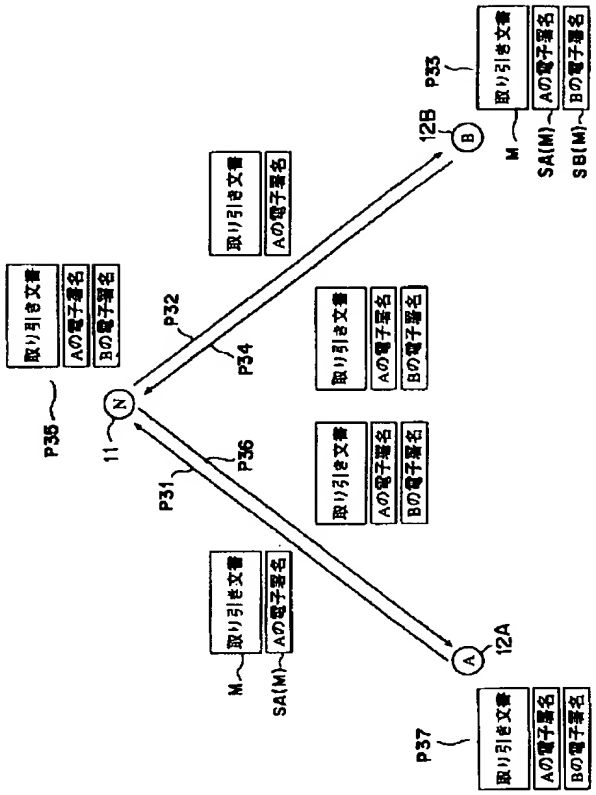
【図１１】

取り引き保証サービスにおける共有情報を示す図



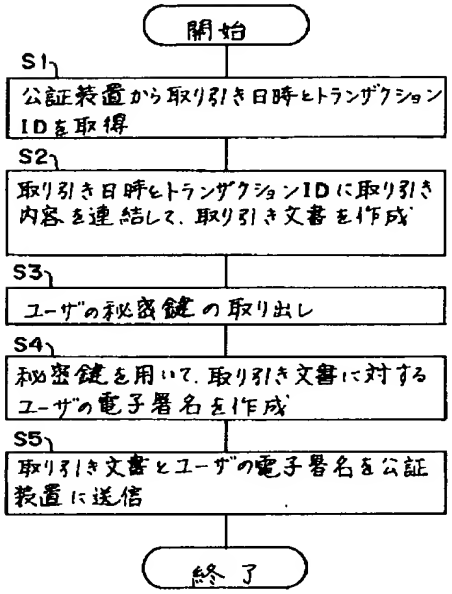
【図１０】

第４の内容保証サービスを示す図



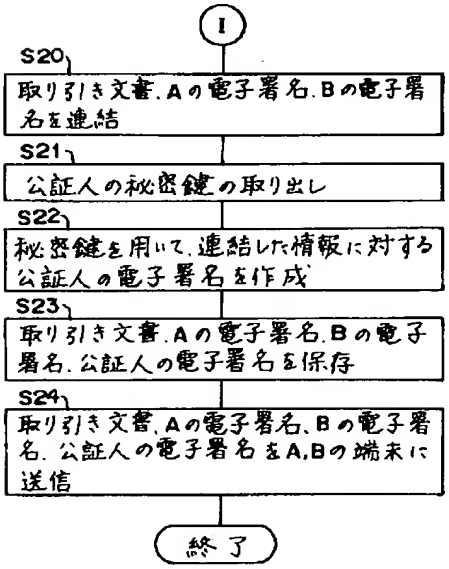
【図１６】

ユーザ端末の第１の処理のフローチャート



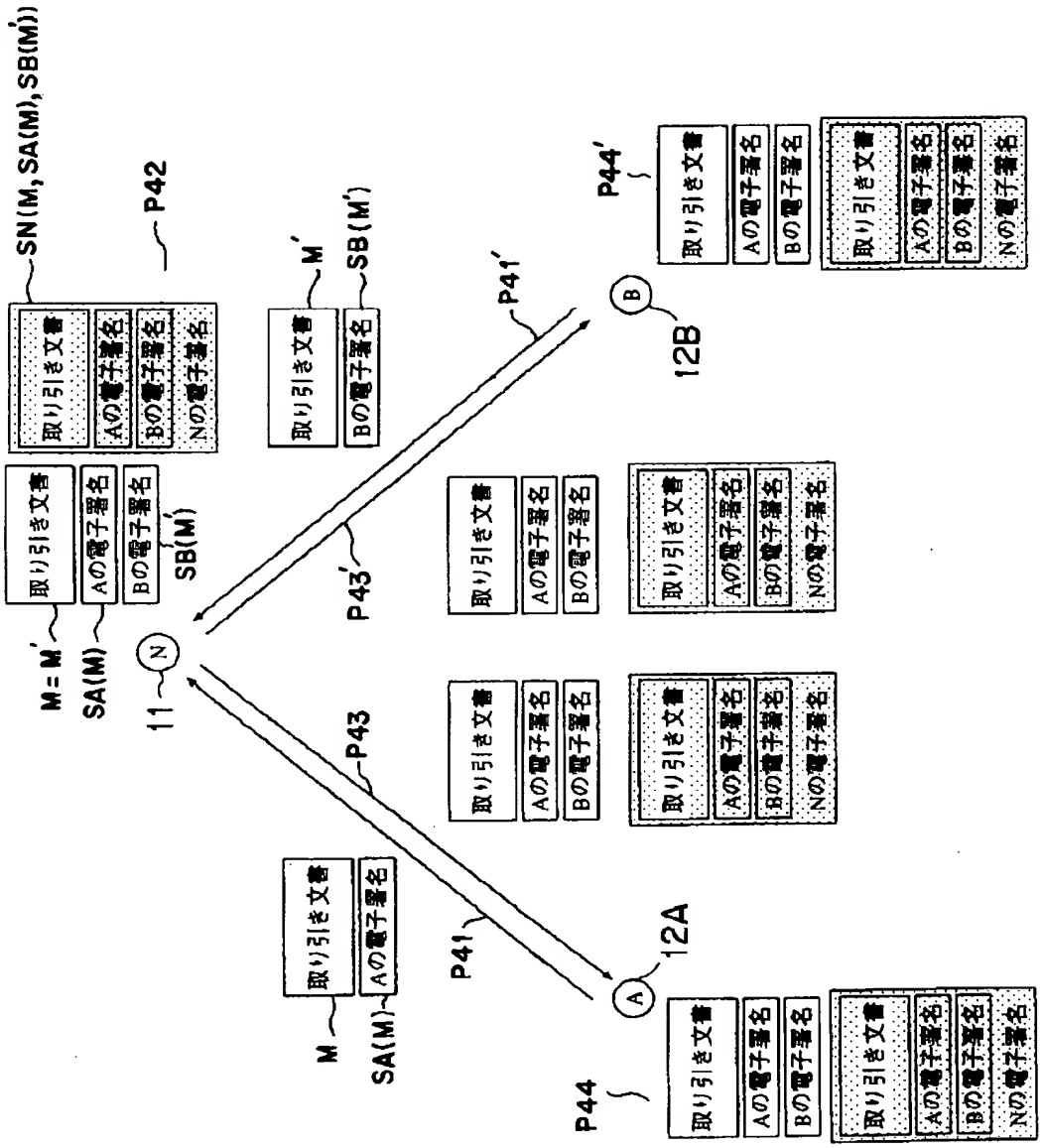
【図１８】

公証装置の処理のフローチャート(その2)



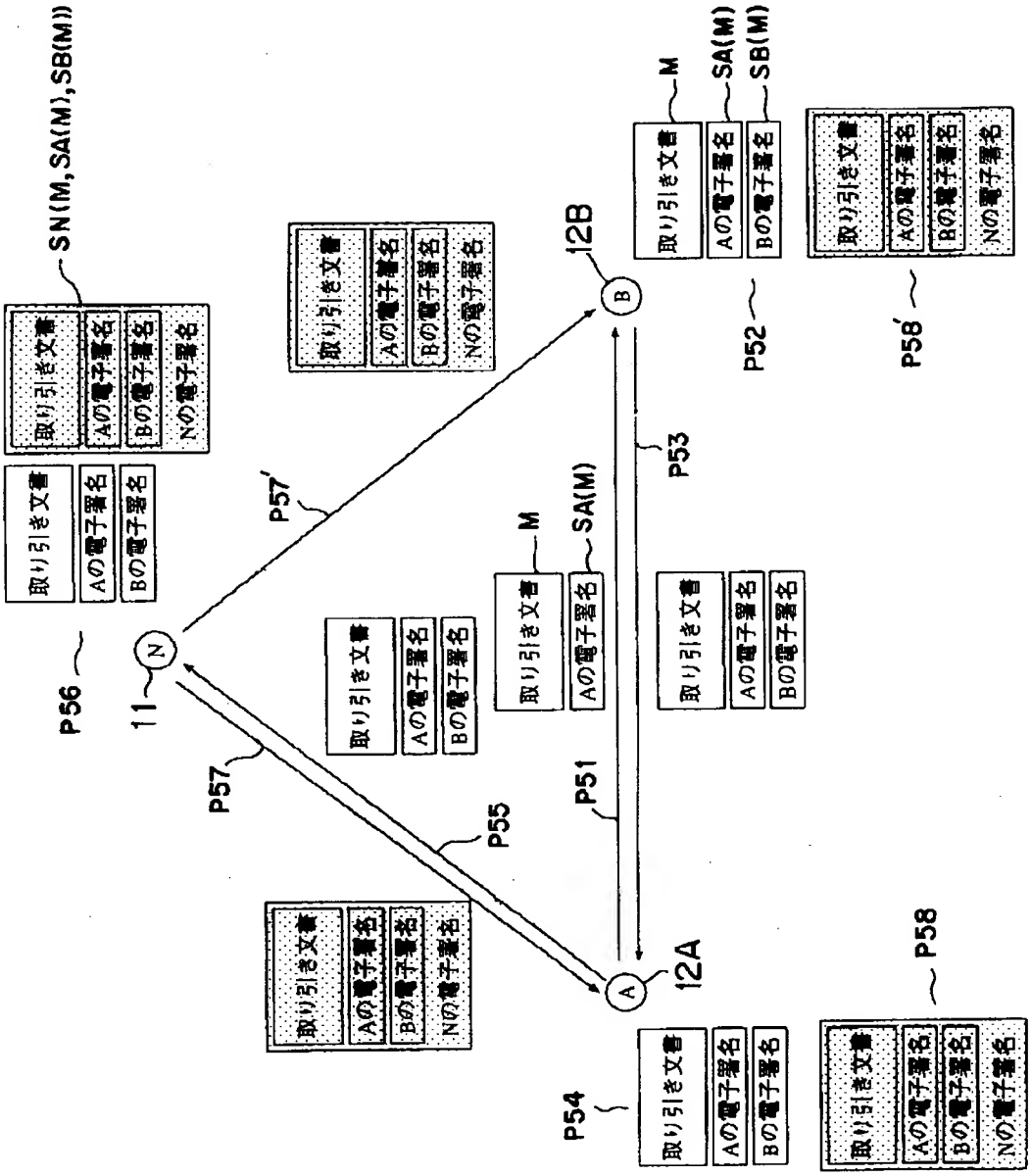
【図１２】

第1の取り引き保証サービスを示す図



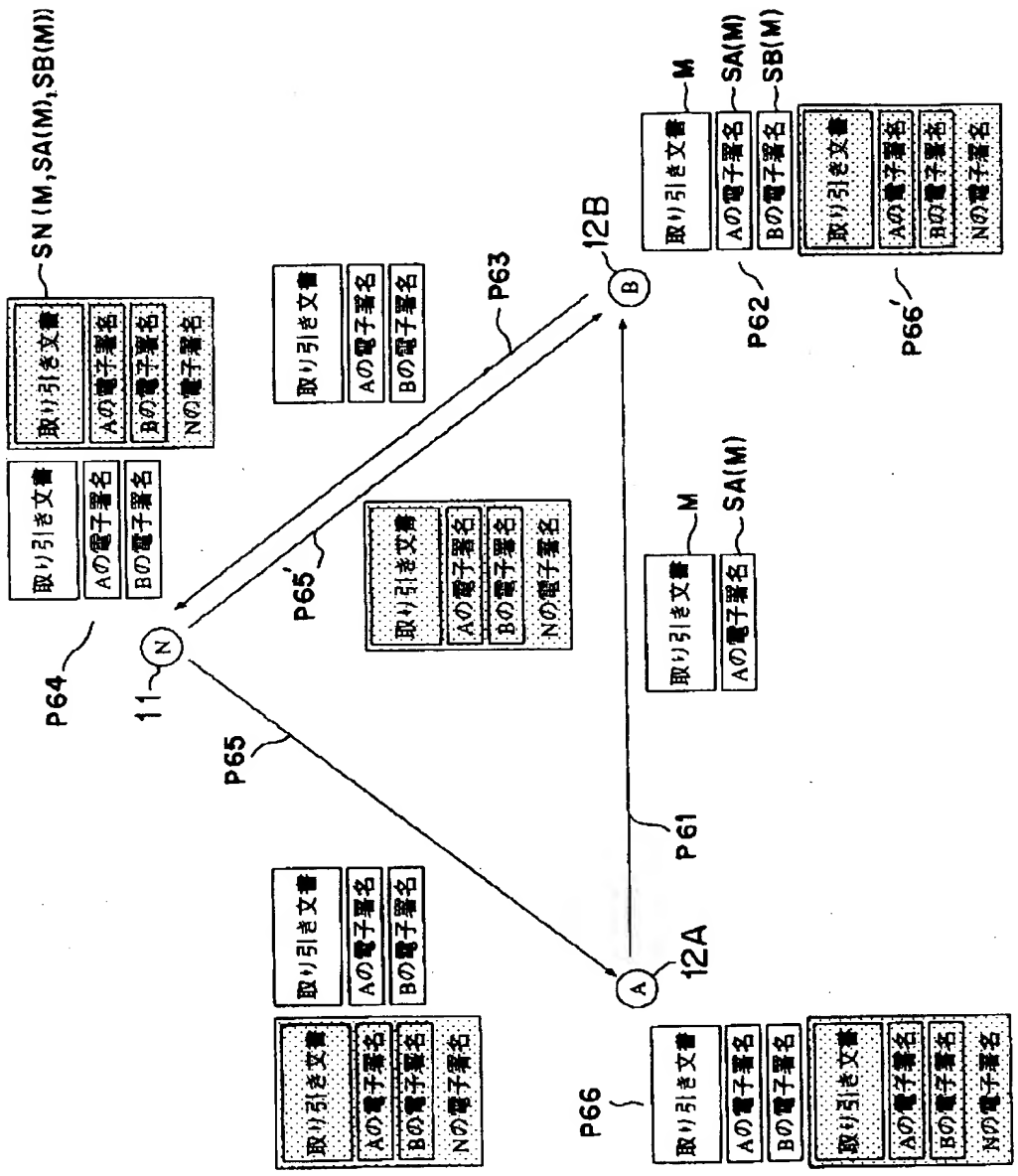
【図１３】

第2の取り引き保証サービスを示す図



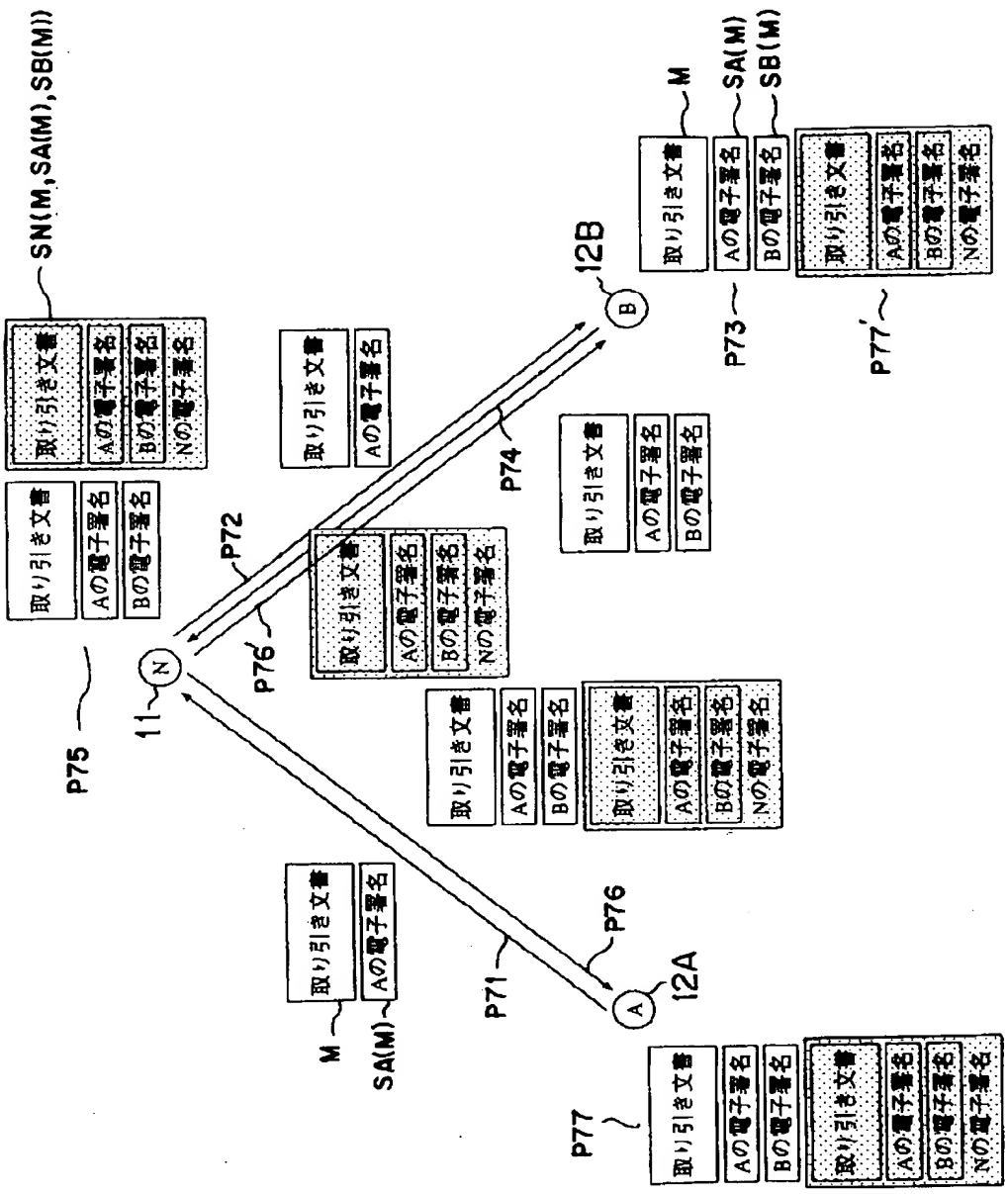
【図１４】

第3の取り引き保証サービスを示す図



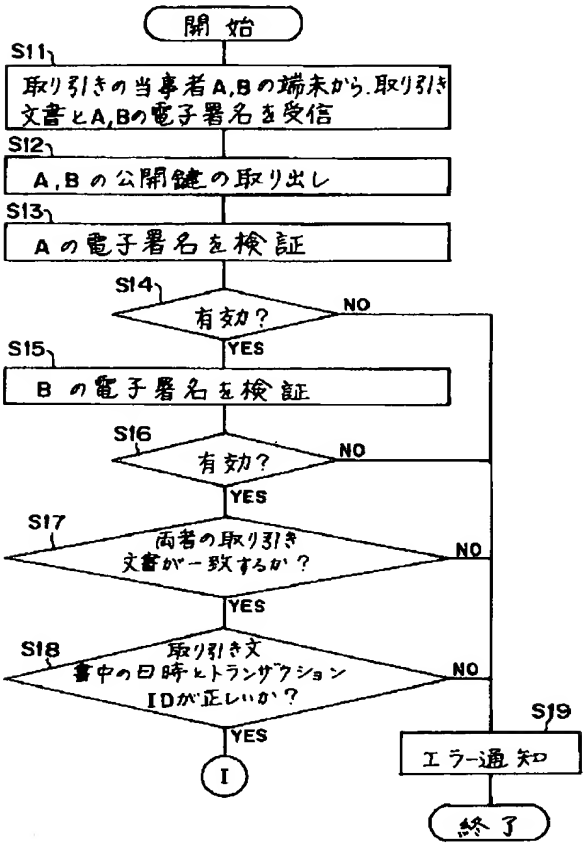
【図１５】

第４の取り引き保証サービスを示す図



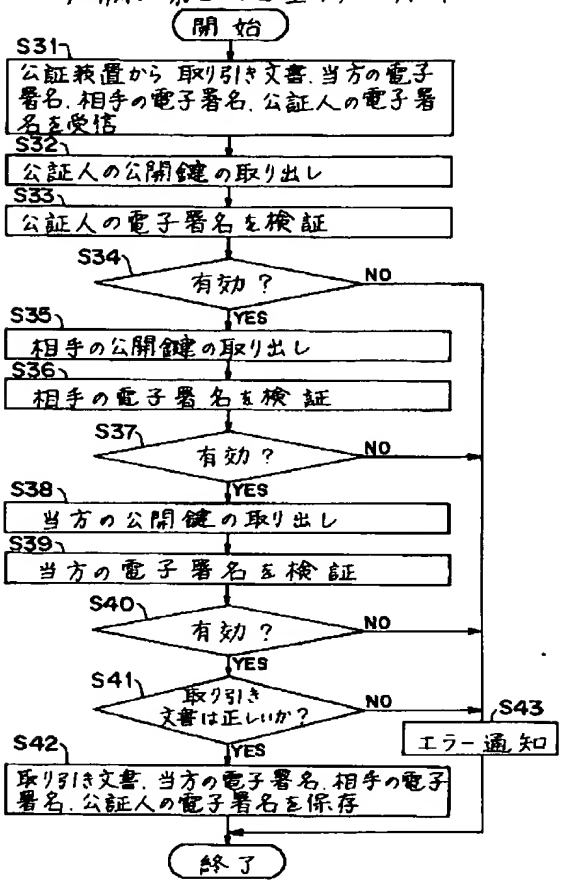
【図１７】

公証装置の処理のフローチャート(その1)

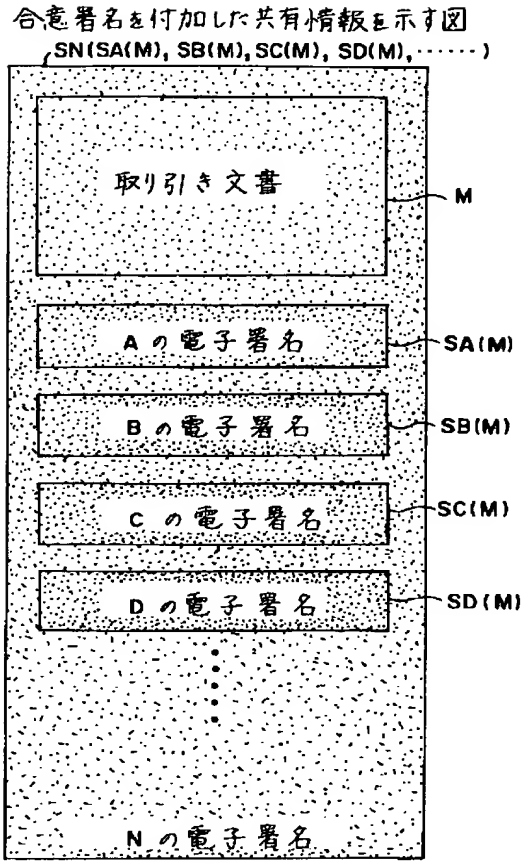


【図１９】

ユーザ端末の第２の処理のフローチャート



【図２１】



フロントページの続き

(72)発明者　鳥居　悟
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　岩瀬　詔子
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　小野　越夫
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内